



**NAVAL
POSTGRADUATE
SCHOOL**

MONTEREY, CALIFORNIA

THESIS

**SECURITY CONCERN IN ACCESSING NAVAL e-
LEARNING WITH PERSONAL MOBILE DEVICES**

by

Keystella R. Mitchell

December 2014

Thesis Co-Advisors:

Man-Tak Shing

Arijit Das

Glenn Cook

Second Reader:

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE
Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

| | | |
|---|---|--|
| 1. AGENCY USE ONLY (Leave blank) | 2. REPORT DATE December 2014 | 3. REPORT TYPE AND DATES COVERED Master's Thesis |
| 4. TITLE AND SUBTITLE SECURITY CONCERNS IN ACCESSING NAVAL e-LEARNING WITH PERSONAL MOBILE DEVICES | | 5. FUNDING NUMBERS |
| 6. AUTHOR(S) Keystella R. Mitchell | | |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000 | | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A | | 10. SPONSORING/MONITORING AGENCY REPORT NUMBER |
| 11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB protocol number <u>N/A</u> . | | |
| 12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited | 12b. DISTRIBUTION CODE A | |
| 13. ABSTRACT (maximum 200 words) | | |
| The purpose of this study was to investigate the feasibility of using personal mobile devices for Naval e-Learning (NeL). Another objective was to find out which mobile device and which method of authentication offers the most practical and secure form of essentially bring your own device (BYOD). The use of personal mobile devices to access NeL is a form of BYOD. Finally, Virtual Desktop Infrastructure (VDI) was examined in this study as another secured means to access NeL from BYOD. | | |
| This study tested the various mobile devices that were Department of Defense (DOD) approved for network use. The study also tested the Common Access Card (CAC) readers that are approved by DOD for CAC authentication against the approved mobile devices. Then the mobile devices and CAC readers' functionality were tested in a VDI environment to examine the various layers of security that could be implemented when using BYOD on DOD networks to maintain the necessary level of information protection. | | |
| The results of this study show the iOS devices were capable of accessing NeL training site via the approved CAC readers. However, the iOS devices could only access and enroll, they were unable to launch training due to Flash not being supported by the native browser, the language used to develop NeL training. The results also revealed attempts to use the iOS device and CAC in a VDI to be unsuccessful as a work around to the Flash issue with the iOS browser. | | |
| The principal conclusion is that through the use of multi-layer security BYOD could be used to access NeL—making it truly available “whenever and wherever.” There is also a need to look into ways authentication can be done without the use of hardware readers. Finally, there is also the need to develop training to support multiple browsers. | | |
| 14. SUBJECT TERMS personal mobile devices, bring your own device (BYOB), Common Access Card, iOS devices, Naval e-Learning (NeL) training, multi-layer security, Virtual Desktop Infrastructure (VDI) | | 15. NUMBER OF PAGES 87 |
| 16. PRICE CODE | | |
| 17. SECURITY CLASSIFICATION OF REPORT Unclassified | 18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified | 19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified |
| | | 20. LIMITATION OF ABSTRACT UU |

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**SECURITY CONCERNS IN ACCESSING NAVAL e-LEARNING WITH
PERSONAL MOBILE DEVICES**

Keystella R. Mitchell
Major, United States Marine Corps
B.S., Clark Atlanta University, 2000

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
December 2014

Author: Keystella R. Mitchell

Approved by: Man-Tak Shing
Thesis Co-Advisor

Arijit Das
Thesis Co-Advisor

Glenn Cook
Second Reader

Dan C. Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The purpose of this study was to investigate the feasibility of using personal mobile devices for Naval e-Learning (NeL). Another objective was to find out which mobile device and which method of authentication offers the most practical and secure form of essentially bring your own device (BYOD). The use of personal mobile devices to access NeL is a form of BYOD. Finally, Virtual Desktop Infrastructure (VDI) was examined in this study as another secured means to access NeL from BYOD.

This study tested the various mobile devices that were Department of Defense (DOD) approved for network use. The study also tested the Common Access Card (CAC) readers that are approved by DOD for CAC authentication against the approved mobile devices. Then the mobile devices and CAC readers' functionality were tested in a VDI environment to examine the various layers of security that could be implemented when using BYOD on DOD networks to maintain the necessary level of information protection.

The results of this study show the iOS devices were capable of accessing NeL training site via the approved CAC readers. However, the iOS devices could only access and enroll, they were unable to launch training due to Flash not being supported by the native browser, the language used to develop NeL training. The results also revealed attempts to use the iOS device and CAC in a VDI to be unsuccessful as a work around to the Flash issue with the iOS browser.

The principal conclusion is that through the use of multi-layer security BYOD could be used to access NeL—making it truly available “whenever and wherever.” There is also a need to look into ways authentication can be done without the use of hardware readers. Finally, there is also the need to develop training to support multiple browsers.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

| | | |
|------|---|----|
| I. | INTRODUCTION..... | 1 |
| A. | BACKGROUND | 1 |
| B. | SCOPE | 2 |
| C. | BRING YOUR OWN DEVICE | 2 |
| D. | CONCERNS WITH BYOD | 3 |
| II. | DOD POLICIES, GUIDELINES AND PLANS FOR MOBILE DEVICE USE..... | 5 |
| A. | DOD COMMERCIAL MOBILE DEVICE IMPLEMENTATION PLAN..... | 5 |
| B. | DOD INFORMATION SECURITY POLICY..... | 6 |
| C. | DEFENSE INFORMATION SYSTEMS AGENCY'S ROLE | 9 |
| D. | DISA'S APPROACH TO APPROVING MOBILE DEVICES..... | 12 |
| E. | APPROVED MOBILE DEVICES | 12 |
| III. | MOBILE DEVICE AND CREDENTIALING REQUIREMENTS..... | 13 |
| A. | MOBILE DEVICES | 13 |
| 1. | Samsung Android..... | 13 |
| a. | Samsung Android KNOX IA Features..... | 13 |
| b. | Samsung Android KNOX Security Features | 14 |
| c. | KNOX Container Configuration | 15 |
| 2. | Apple iOS 6..... | 18 |
| a. | iOS Security Features | 18 |
| b. | iOS Provisioning and Setup..... | 19 |
| c. | Application Management..... | 20 |
| d. | Wi-Fi and Bluetooth Use | 20 |
| e. | iOS Browser Requirements..... | 20 |
| B. | ACCESS CONTROL METHODS..... | 22 |
| 1. | Identification Credentials..... | 23 |
| 2. | Authentication | 23 |
| 3. | Authorization..... | 25 |
| 4. | Vulnerability Category Codes | 26 |
| 5. | Logical Method..... | 26 |
| a. | Password..... | 26 |
| b. | Public Key Infrastructure | 28 |
| c. | DOD Common Access Card | 30 |
| d. | The Process of the Biometric System | 31 |
| 6. | Enrollment into the Biometric System..... | 32 |
| a. | Verification of the Biometric System..... | 33 |
| b. | Separation of Duties in the Biometric System | 33 |
| IV. | TESTING AND EVALUATION..... | 37 |
| A. | TESTING SCENARIOS | 37 |
| 1. | iOS and PKard Smart Card Readers..... | 37 |

| | | |
|---|--|-----------|
| a. | <i>Attempts to Launch Training</i> | 45 |
| 2. | iOS and baiMobile Smart Card Reader | 46 |
| B. | EVALUATION OF TESTING | 48 |
| V. | CONCLUSION AND FUTURE RESEARCH | 51 |
| A. | CONCLUSION | 51 |
| B. | FUTURE RESEARCH | 51 |
| 1. | Continued Testing of Approved Mobile Devices and Methods | 51 |
| 2. | Support of Multiple Browsers | 51 |
| 3. | Support of CAC Enable Sites via VMware | 52 |
| 4. | Support of Soft Certification | 52 |
| 5. | Classification of Information | 52 |
| 6. | Hosting a .Com Site | 52 |
| C. | SUMMARY | 52 |
| APPENDIX A. SAMSUNG ANDROID WITH KNOX 1.X V2R1 OVERVIEW | | 55 |
| APPENDIX B. SAMSUNG ANDROID WITH KNOX 1.X V2R1 CONFIGURATION TABLE | | 57 |
| APPENDIX C. APPLE IOS 6 VPN CONSIDERATIONS | | 65 |
| LIST OF REFERENCES | | 67 |
| INITIAL DISTRIBUTION LIST | | 69 |

LIST OF FIGURES

| | | |
|------------|--|----|
| Figure 1. | UC High-Level Operational Framework (from DOD, 2013) | 10 |
| Figure 2. | Framework for Samsung Android with KNOX 1.x (from Samsung, n.d.)..... | 18 |
| Figure 3. | Notional DOD iOS 6 Connection (from DISA, 2013) | 21 |
| Figure 4. | Layered Protection of Logical Asset (from DISA, 2010)..... | 22 |
| Figure 5. | General Illustration of CAC Layout (from DOD, n.d.) | 31 |
| Figure 6. | Notional Example of Leveraging Logical Security Services (from DISA, 2010) | 35 |
| Figure 7. | Plug-in and Case CAC Readers or the iOS (from thursby.com) | 38 |
| Figure 8. | Screen Capture of the Application Used for the PKard Reader..... | 39 |
| Figure 9. | Screen Capture of the Import of DOD Sites | 39 |
| Figure 10. | Screen Capture of the U.S. Navy Sites | 40 |
| Figure 11. | Screen Capture of NKO Site..... | 41 |
| Figure 12. | Screen Capture of Client Certificates | 41 |
| Figure 13. | Screen Capture of Authentication Request | 42 |
| Figure 14. | Screen Capture of NETC Learning Management System site..... | 43 |
| Figure 15. | Screen Capture of Course Catalog NETC LMS site..... | 44 |
| Figure 16. | Screen Capture of Enrollment into a Course NETC LMS site | 44 |
| Figure 17. | Screen Capture of Confirmed Enrollment on NETC LMS site | 45 |
| Figure 18. | 3000 MP Bluetooth Smart Card Reader (from biometricassociates.com)..... | 46 |
| Figure 19. | 301MP LT Smart Card Reader (from biometricassociates.com)..... | 47 |

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

| | | |
|----------|---|----|
| Table 1. | Potential Impact Definitions for Security Objectives (from NIST, 2004)..... | 8 |
| Table 2. | DOD Approved Mobile Devices (from DISA, n.d.-b) | 12 |
| Table 3. | Samsung's KNOX recommended container configuration (from Samsung & DISA, 2014a) | 17 |
| Table 4. | Authentication Methods (after DOD, 2010) | 24 |
| Table 5. | Vulnerability Severity Code Definitions (from DOD, 2010) | 26 |
| Table 6. | Test Matrixes for NeL Site | 49 |

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS

| | |
|-------|--|
| BYOD | bring your own device |
| C2 | Command and Control |
| CAC | Common Access Card |
| CIO | chief information officer |
| CMD | commercial mobile device |
| CUI | Controlled Unclassified Information |
| DAA | designated accrediting authority |
| DISA | Defense Information Systems Agency |
| DISN | Defense Information Systems Network |
| DOD | Department of Defense |
| DODD | Department of Defense Directive |
| DON | Department of Navy |
| DTS | Defense Travel System |
| FIPS | Federal Information Processing Standards |
| FOUO | For Official Use Only |
| IA | information assurance |
| IE | Internet Explorer |
| JIE | Joint Information Environment |
| LMS | Learning Management System |
| MAM | Mobile Application Management |
| MAS | mobile application store |
| MDM | Mobile Device Management |
| MEM | Mobile Email Management |
| NCCoE | National Cybersecurity Center of Excellence |
| NETC | Navy Education and Training Command |
| NeL | Navy e-Learning |
| NIST | National Institute of Standards and Technology |
| NKO | Navy Knowledge Online |
| OS | operating system |
| OTA | over-the-air |

| | |
|------|---------------------------------|
| OV | operational view |
| PIV | personal identity verification |
| PKI | public key infrastructure |
| SAFE | Samsung Approved For Enterprise |
| UC | unified capabilities |
| VM | virtual machine |
| VPN | Virtual Private Network |

ACKNOWLEDGMENTS

I would like to thank God for all that I am and all that I could be. For if it was not for God, I know not where I would be. I would like to thank Mom and Dad for their love and understanding and raising me to believe that through hard work and continuous prayer there is nothing that I cannot achieve. To my family and close friends I would like to thank you for your prayers and words of encouragement. To my sons, Fredrick Jr. and Roddrick, you are my inspiration to continue to aspire to be and do better. To Fredrick, my husband, my love, my motivation, and my strength, I cannot thank you enough for keeping me focused on my purpose—I love you.

For those whom God has placed in my path I say thank you: CDR Blassingame for when I was frustrated and wanting to give up you gave me words of encouragement that helped me to pull it together to start and complete the work on this thesis; Dr. Shing, Mr. Das, and Mr. Cook for working with me to help develop and organize my thoughts. I would also like to thank Erik Lowney for his assistance with setting up and testing of the virtual environment. Last, but not less, Colonel McCarthy and Lieutenant Colonel Raffetto for their quick response to help with getting the additional time to necessary to complete my thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

As part of the Navy's goal to make Navy training accessible "whenever and wherever," the Navy Education and Training Command (NETC) and Sea Warrior Program Office has made the content of Navy e-Learning (NeL) directly accessible from the Internet (Barker, 2014). There is no longer the need to access Navy Knowledge Online (NKO) in order to gain access to the learning management system NeL.

NeL is an educational portal resource that hosts learning and training for Sailors, government civilians, and contractors, and it is used by active duty, reserve, and retired enlisted and officers for both personal and professional use. Since its inception in 2001, this has been the Navy's way of keeping the lines of communication and sharing open between active, reserve and retired personnel. NeL offers more than 8,700 courses annually. It is boasted that there are more than four million courses completed via NeL yearly (Baker, 2014).

NeL utilizes the latest version of Internet Explorer (IE) and requires a Common Access Card (CAC) to login. A CAC is required as part of the *Information Assurance* (IA) policy instituted by the Department of Defense (DOD) 8500.01E. This limits potential users from being able to access NeL from various mobile devices "whenever and wherever." NeL is also expected to maintain a high level of security due to the type of information being accessed via the Internet.

Until the Navy is comfortable with the level of security that can be achieved via personal secure mobile devices (e.g., smartphones and tablets) as well as updating browser compatibility the goal of "whenever and wherever" will not be realized. In large part, this is because of the need to maintain a heightened level of security for the type of information that could be potentially transmitted via mobile devices. This is due to the nature of personal mobile devices continuously left on and always in one's possession, which makes them susceptible to being lost or stolen and the information stored within fall into the wrong hands. This same argument can be made for Blackberries, which are

government owned and issued; however, the protective measures include two key factors 1) the government owns the information stored within 2) should the device be compromised the government can remotely shut down and swipe the device once notified.

There is current technology and safeguards available, similar to those used for government owned devices that could be implemented to secure personal mobile devices. This thesis will address some of the technologies and safeguards currently available that could potentially bring the Navy closer to the realization of the goal “whenever and wherever” NeL training.

B. SCOPE

For the purpose of this thesis, training pertains strictly to electronic learning. The study will identify the policies, guidelines, strategies, and plans. It will also evaluate and rank those mobile devices and readers necessary to support a secure connection from personal secure mobile devices to an unclassified Naval e-Learning web portal for the purpose of providing NeL whenever and wherever. The study will define the term bring your own device (BYOD) and then identify concerns/issues with the use of BYOD. Chapter II discusses the current DOD polices, plans, governance established for mobile devices also known as mobile computing, and Defense Information Systems Agency’s (DISA) role in DOD use of mobile devices. Chapter III identifies the approved mobile devices configuration requirements, the various types of credentialing methods available for secure authentication, and the system architecture for mobile computing. Chapter IV presents a proof of concept study to evaluate the capabilities of approved mobile devices and readers necessary to make a secure connection to the NeL site for the purpose of enrolling and launching a training session. Chapter V provides the conclusion and offers future recommended research.

C. BRING YOUR OWN DEVICE

The definition of BYOD is the practice where employees bring their own personal mobile computing devices into the workspace for use on the company’s network. The mobile devices include, but are not limited to smartphones, tablets, and personal data

assistants. The demand for BYOD within the workforces is becoming more and more popular because of the advancements in technology. These devices are smaller, light weight, easily accessible and in some instances offer the same/similar computing power as a traditional laptop or desktop.

D. CONCERNS WITH BYOD

The number one concern with BYOD is security. Due to existing policies, operational construct and security vulnerabilities currently there is not an executable DOD BYOD plan (Department of Defense, 2013). The Defense Information Systems Agency, along with other DOD components, is looking at trying to close the gap with the use of Virtual Desktop Infrastructure (VDI) technology. This is an area that is being closely monitored by the CIO for implementation in conjunction with the *Digital Government Strategy* (Department of Defense [DOD], 2013).

THIS PAGE INTENTIONALLY LEFT BLANK

II. DOD POLICIES, GUIDELINES AND PLANS FOR MOBILE DEVICE USE

The DOD Chief Information Officer (CIO) stated in the May 2012 roll out of the DOD *Mobile Device Strategy* that it is not just about embracing the latest technology but more about keeping the Department's workforce relevant when it comes to critical roles cybersecurity and information accessibility plays in today's mission accomplishment. The DOD lags behind in keeping pace with technology and the ability to access information whenever and wherever necessary. In an effort to try and remedy this issue, the DOD *Commercial Mobile Device Implementation Plan* was released February 2013.

A. DOD COMMERCIAL MOBILE DEVICE IMPLEMENTATION PLAN

The DOD (2013) *Commercial Mobile Device* (CMD) plan is a phased approach to implementing mobile secure classified and protected unclassified information while utilizing commercial off-the-shelf technology. The leading agency for the implementation of this plan is the Defense Information System Agency (DISA).

The Defense Information Systems Agency has been tasked with developing an enterprise solution, which promotes mobile Controlled Unclassified Information (CUI) conditions necessary to support utilizing commercial carrier infrastructure while providing an entry point for classified services. The DOD (2012b) Instruction 5200.01 defines CUI as unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable laws, regulations and government-wide policies. This along with unclassified information, will be addressed in this study although, the CMD plan covers both secure classified and protected unclassified mobility requirements. In particular this study will focus on the use of personally owned and operated devices while maintaining security of protected unclassified information.

The vision of the CMD plan is to develop a framework, which will capitalize on the goals of the *Mobile Device Strategy* by exploiting mobile device technologies in order to achieve information technology mobility goals (DOD, 2012a). These goals, as identified in the *Mobile Device Strategy*, are to develop a wireless infrastructure, utilize current mobile devices, and develop DOD approved mobile applications. This study will touch on each of the identified goals with a focus on the mobile device itself. This plan is designed to support a device-agnostic approach for the CMD environment. This approach is in an effort to support a variety of operational use case scenarios.

B. DOD INFORMATION SECURITY POLICY

In order to achieve the vision of the CMD plan it is necessary that particular attention be paid to information security. Due to this being somewhat uncharted territory for the DOD, the development of wireless mobility architecture will live and die by the security of the information that transverse its network.

In general the purpose of DOD manual 5200.01, volume 1 (2012c) states that it is to implement policy, assign responsibilities, and provide procedures for the designation, marking and protection, and dissemination of CUI and classified information including information categorized as collateral sensitive compartmented information, and special access program. The focus will be on the protection of unclassified information and CUI.

Although a larger majority of DOD's business is conducted on the Non-secure Internet Protocol Router Network (NIPRNet) in the unclassified domain there still exist the requirement for all DOD unclassified information to be reviewed and approved for release through standard DOD component processes before it is provided to the public in accordance with Department of Defense Directive (DODD) 5230.09 *Clearance of DOD Information for Public Release* (DOD, 2012c). This is primarily for the purpose of maintaining operation security. This is accomplished by the use of standards developed by NIST. The standard used for security categorization of information and information systems is the Federal Information Processing Standards (FIPS) Publication 199.

The Federal Information Security Management Act of 2002 (Public Law 107-347) defines three security objectives for information and information systems as the following:

- Confidentiality: “Preserving authority restriction on information access and disclosure, including means for protecting personal privacy and proprietary information...” (44 U.S.C., Sec. 3542). A loss of confidentiality is the unauthorized disclosure of information.
- Integrity: “Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity...” (44 U.S.C, Sec. 3542). A loss of integrity is the unauthorized modification or destruction of information.
- Availability: “Ensuring timely and reliable access to and use of information...” (44 U.S.C., Sec. 3542). A loss of availability is the disruption of access to or use of information or an information system.

The FIPS 199 defines the impact that a breach of either of the above security objectives would have on the organization or individuals. Table 1 summarizes the potential impact at low, moderate, and high levels on each of the identified security objectives.

Table 1. Potential Impact Definitions for Security Objectives
(from NIST, 2004)

| Security Objective | POTENTIAL IMPACT | | |
|--|---|---|--|
| | LOW | MODERATE | HIGH |
| Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary [44U.S.C., SEC. 3542] | The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |
| Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542] | The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals | The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |
| Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542] | The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |

C. DEFENSE INFORMATION SYSTEMS AGENCY'S ROLE

The Defense Information Systems Agency is essentially the DOD's gatekeeper for networked information. The mission and vision of DISA per its website is to be a:

Combat Support Agency, that provides and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint Warfighters, National level leaders, and other mission and coalition partners across the full spectrum of operations. (DISA, n.d.-a)

Its vision is simply, "Information superiority in defense of the Nation" (DISA, n.d.-a).

Defense Information Systems Agency offers a multitude of services to its mission partners; the following are few of the services that are provided.

- Command and Control (C2)
- Computing
- Contracting
- Enterprise Engineering
- Enterprise Services
 - Applications
 - Infrastructure
 - Identity and Access Management
- Information Assurance
- Network Services (Defense Information Systems Network [DISN])
 - Data
 - Voice
 - Video
 - Messaging
 - Wireless
 - Satellite
- Spectrum
- Testing (DOD, 2012a)

This list serves as the basis behind the unified capabilities (UC) concept. It will provide as the widespread continuous UC at the high level of operational concept for any user whenever and wherever on any device. Figure 1 depicts the overarching UC operational concept model (OV-1).

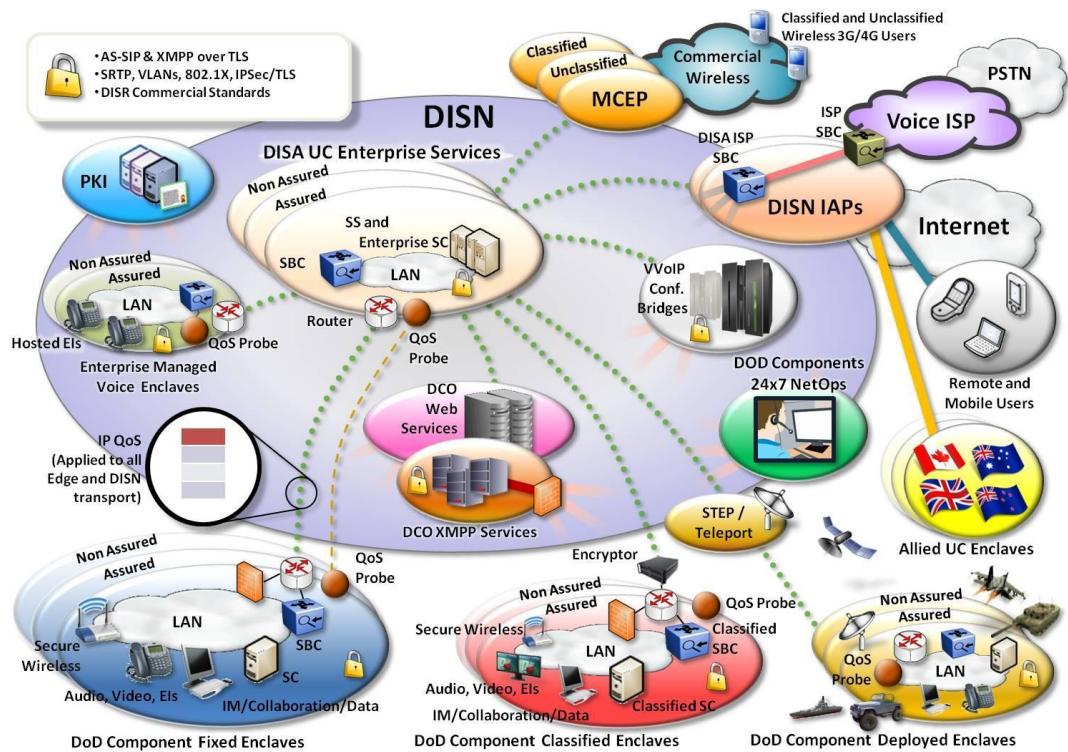


Figure 1. UC High-Level Operational Framework (from DOD, 2013)

This can only be achieved through a dynamic and robust method of information sharing. The Defense Information System Agency is looking to achieve this type of information sharing for DOD and other federal agencies for enterprise-level secure and protected off the shelf mobility solution through development of a seven-focus area approach. This will be accomplished through the DOD Mobility Program of which DISA is the lead agent.

Mobility serves as the key enabler to allowing mission partners to connect to the Joint Information Environment (JIE) “whenever and wherever” via authorized mobile

devices. DOD and DISA are looking to establish policies and procedures to advance information sharing, collaboration, and efficiencies through the use of secure mobile technologies with security and performance as their primary goals.

The DOD (2012a) *Mobile Device Strategy* has laid out four mobility goals for DISA to achieve:

- Goal 1: Advance and Evolve the DoD Information Enterprise Infrastructure to support Mobile Devices;
- Goal 2: Institute Mobile Device Policies and Standards;
- Goal 3: Promote the Development and Use of DoD Mobile and Web-Enabled Applications;
- Goal 4: Develop and Enterprise Mobility Service for Classified and Unclassified Capabilities (Department of Defense, 2012a).

Mobility is no longer seen as a luxury—it has become a requirement and as the Program Management Office for mobility has developed a phased approach to identify, adopt, and securely implement a mobile solution.

Phase 1: Nov. 2012–Apr. 2013 (The Unclassified Mobility Pilot)

- Establish a multi-vendor mobile capability within DOD for assessment
- Deploy voice and data services over a commercial wireless network
- Award a contract for DOD enterprise MDM and MAS

Phase 2: Apr.–Sept. 2013 (Pilot Expansion and Transition)

- Establish a network infrastructure to support the user community
- Deploy mobile devices to Military Service and Combatant Command users

Phase 3: Oct. 2013 and beyond (Operational Capability)

- Mobility becomes an operational capability offered to the DOD enterprise as a subscription service
- Enterprise contracts to support data plans and purchase of approved devices will be established. (DISA, n.d.-a)

The DISA's mobility foundation is built on the implementation and integration of the Mobile Device Manager (MDM), Mobile Application Store (MAS), and Mobile Virtual Private Network (MVPN) to provide secure and reliable services to the warfighter and other federal employees whenever wherever. This foundation aids in closing the technology gap that exists in DOD by offering a network infrastructure that boosts

delivery of 3G and 4G LTE services in order to extend UC. This approach provides DOD with an enterprise solution at a significant savings, while eliminating duplication and promoting economies of scales.

D. DISA'S APPROACH TO APPROVING MOBILE DEVICES

In an effort to keep pace with current technologies while maintaining a level of security necessary to protect the nation's networks, DISA has streamlined to the device approval process. This streamlined approach consists of five steps: (1) DISA identification of IA requirements; (2) industry development of a device with a Security Technical Implementation Guide (STIG) in accordance with the IA guidance; (3) simultaneous delivery of device and STIG; (4) DISA review of device and STIG for compliance; and (5) device approval for DOD use in conjunction with release to commercial market ("Secure Unclassified," n.d.).

A STIG is a standardized secure methodology implemented by DISA for installing and maintaining hardware and software for computers. It is implemented on all DOD computing devices for security purposes locking down the device to protect against vulnerabilities.

E. APPROVED MOBILE DEVICES

To date DISA has approved the following mobile devices and operating systems, listed in Table 2.

Table 2. DOD Approved Mobile Devices (from DISA, n.d.-b)

| OPERATING SYSTEMS | SMARTPHONES | TABLETS |
|--------------------------|-----------------------------|---|
| Apple iOS (7.1.x) | iPhone 4, 4S, 5, and 5S | iPad Mini, 2, 3, and 4 iPad Mini-R iPad Air |
| Android OS (4.4.x) | Samsung Galaxy S4 with KNOX | |

III. MOBILE DEVICE AND CREDENTIALING REQUIREMENTS

A. MOBILE DEVICES

The following mobile devices have been tested and approved by DISA the DOD Mobility Program Management Office.

1. Samsung Android

On May 3, 2013, DISA approved the first release of Android/Samsung KNOX 1.x capability. The 2.x version was approved for release on May 9, 2014. The STIG supports KNOX 1.x version, which supports MDM for secure access to DOD networks. It also supports Defense Enterprise Email and For Official Use Only (FOUO) environment calendar and contact synch capability. The operating system (OS) offers access to the 19 tested and approved applications currently offered at the Mobile Application Store (MAS). Features such as Wi-Fi, GPS, Bluetooth, native browser, contacts, and device encryption are also offered on the mobile device.

These features were made possible by Samsung development and approval of the STIG that supports its KNOX capability. The KNOX is a security feature that allows both a personal and work environment to exist together on a single mobile device. This security feature is achieved by a method identified as “container.” It is a part of Samsung Approved For Enterprise (SAFE) approach to providing a more secure smartphone and tablet (Samsung & DISA, 2014a).

a. *Samsung Android KNOX IA Features*

Samsung offers the following IA features, which aid in developing the secure environment through multi-layer security necessary to access a DOD network.

- Mobile Application quarantine
- Smart Card support
- Host-based firewall
- Ability to revoke mobile application permissions
- Over-the-Air (OTA) audit log retrieval

- Support for PKI authentication and certificate verification in native browser (Samsung & DISA, 2014a)

The Samsung Android Platform that supports these IA features is an extension of the Android 4.1.1 SELinux-enabled kernel, which supports the SAFE technology that allows the use of MDM control. Samsung KNOX 1.0 is support by Samsung Galaxy S3, S4 and Android 4.2.2 and 4.3 in the Galaxy Note 2 and 3 (Samsung & DISA, 2014).

b. Samsung Android KNOX Security Features

The Samsung Android features a dual workspace environment made available through the KNOX technology, which is based on compartmentalizing the various workspaces into their own secure isolated containers. This is made possible by the following security features:

- Separate home screen, launcher, applications and widgets.
- AES 256 encryption of all container data using a FIPS 140-2 validated cryptographic module.
- No interaction between applications and data inside and outside the container.
- Password based access control mechanism that is independent of the device lock screen.
- Data in transit protection of all container network traffic using a VPN employing FIPS 140-2 validated cryptographic modules.
- Container only configuration and management policies including application management, password complexity, CAC configurations for browser and email, and remote wipe of only the container (Samsung & DISA, 2014a).

According to DISA “As a device owned and issued by DOD the guidelines for use falls under the terms of the DOD Information Systems User Agreement therefore there is no expectation of privacy when utilizing the device regardless of the workspace environment” (Samsung & DISA, 2014). For more information on the details of the container technology and expected use when on a DOD network see Appendix A.

c. KNOX Container Configuration

The KNOX container is configured to be controlled by the MDM through policies set in the STIG, separate and independent of those of the device. The following container policies, as well as the STIG policies, are available giving full access to the administrator.

(i) Container Management Policies

The controls for management allow the administrator to:

- Create one container per device
- Remove container and all content
- Lock/unlock container as determined

(ii) Container Application Management Policies

The MDM administrator is able to control all the applications the user downloads and installs from the Samsung KNOX application store via the below policies:

Package Whitelist the MDM has the authority to add and remove packages in the Whitelist and if configured only applications in the Whitelist can be installed in the container.

- Install/Uninstall applications in the container
- Enable/Disable applications in the container and users are blocked from disabled applications.
- Start/Stop applications remotely inside the container.

(iii) Container Password Policies

Samsung password policies allow the MDM the same controls as those administered on the DOD network the administrator has the following authorizations to:

- Set the maximum number of failed attempts before being disabled
- Set expiration of container password
- Set minimum length requirement
- Set idle time before a container will lock

- Set the number of previous passwords in history to prevent against reuse
- Set the minimum number of characters that are required to be changed when changing a password
- Set the complexity of a password (e.g., uppercase, lowercase, numeric, and special characters)

(iv) Container Email and Browser Policies

The MDM has the following controls for configuration of the native email and browser applications.

- Set the proxy
- Enable/disable JavaScript
- Enable/disable cookies
- Enable/disable Smartcard authentication
- Whitelist/blacklist accounts allowed in email according to domain name
- Enable/ disable Smartcard (CAC) credentials on specific accounts (Samsung & DISA, 2014a)

(v) Recommended Configuration

Table 3 is a recommended configuration setting for MDM by Samsung to demonstrate how the container can be made secure.

Table 3. Samsung's KNOX recommended container configuration (from Samsung & DISA, 2014a)

| Policy | Setting | Description |
|----------------------------------|--------------------------------------|--|
| Application Whitelist | Enterprise Whitelist of Applications | Only those applications on the Whitelist can be installed from the KNOX App Store |
| Minimum password length | 6 | Container password must be at least 6 characters |
| Password quality | Complexity | Password must contain letters, numbers and special characters |
| Maximum time to lock | 15 min | Container will auto-lock after 15min of inactivity |
| Minimum character change length | 2 | User must change at least 2 characters when changing the password |
| Maximum failed password attempts | 3 | Container will be admin locked when the user fails to enter the correct password on 3 attempts |
| Set http proxy | DOD proxy address | All browser traffic will be directed to the DOD proxy server |
| Account Whitelist | Enterprise email address domain | Only enterprise email accounts will be allowed inside the container |
| Browser Smartcard authentication | Enable | Enable Smartcard authentication for browser |
| Email Smartcard credentials | Enable/DOD email account | Enable Smartcard credentials for specified email accounts |

For a more complete listing of the Samsung Android (with KNOX 1.x) STIG configuration see the table of configuration in Appendix B. Figure 2 is a pictorial representation of the framework for both the normal and KNOX container workspace in the Samsung Android.

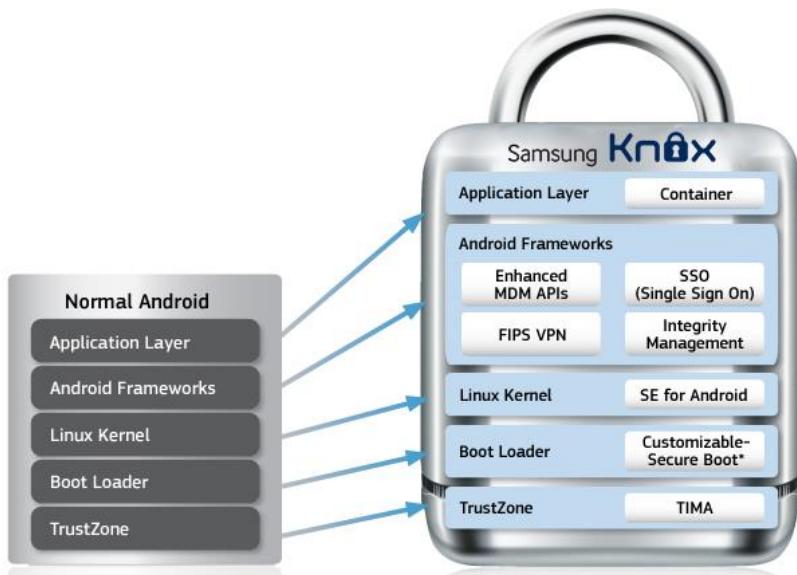


Figure 2. Framework for Samsung Android with KNOX 1.x
(from Samsung, n.d.)

2. Apple iOS 6

On May 17, 2013, DISA officially announced the approval of the STIG for Apple's iOS6 operating system. With this approval, and the MDM in place, DISA was able to run a pilot program allowing the secure use of commercial mobile devices on the DOD network.

The approval included use with the iPhone 4S, iPad2, iPad Mini, and later models of the iOS operating system approved by DOD. This approval however excludes the iPod touch devices because it does not support the trusted boot process in the iOS operating system.

a. *iOS Security Features*

The STIG requires the use of a third-party product in order to provide the following required security features:

- Mobile Device Management (MDM)
- Mobile Application Management (MAM)
- Mobile Device Integrity Scanning (MDIS) capability that allows the MDM administrator to scan the device for vulnerabilities

- Mobile Email Management (MEM) capability manages the DOD email and acts as interface between email server and device
- Security container for offers FIPS 140-2 the security requirements for cryptographic module used in protecting sensitive but unclassified information
- iOS 6 cryptographic module is FIPS 140-2 validated
- The DOD browser must be installed inside the security container
- CAC reader and middleware. (DOD, 2013)

The STIG offers the flexibility to use varying products to meet the needs of the command, meaning as long as the product meets all the specified STIG requirements and documented configuration settings for that server then the products can be mixed or matched.

b. iOS Provisioning and Setup

The provisioning and setup will vary from device to device depending on the MDM used this is for DOD issued devices. The following is a general guideline for provisioning and setup:

- Device activation follow on-screen prompt
- Install MDM
- Activate MDM and install DOD security profile
- Download apps from MAS
- Configure CAC
- Setup iOS restriction
- Turn off iMessage (not authorized)
- Turn off Wi-Fi and Bluetooth they can be enable as needed
- App Store and iTune Music Store disabled by MDM server (DOD, 2013)

User must complete required training and sign a user agreement prior to receiving the mobile device.

c. Application Management

Due to the malware risk associated with applications it is recommended that the following procedures be utilized for review and management of device applications prior to DISA's App Store being made available to new users

- Designated Accrediting Authority (DAA) setup a review process for all apps using the MA SRG as the required documentation for review
- Obtain an enterprise code signing identity from Apple.
- This will allow apps to be signed with an Apple-provide key where developed by DOD or by a commercial vendor.
- All approved apps are to be managed via the MAM server or a command sponsored app store. (DOD, 2013)

d. Wi-Fi and Bluetooth Use

The iOS device does not support FIPS 140-2 cryptographic validation for Wi-Fi or Bluetooth and does not support authentication via CAC or personal identity verification (PIV); therefore, the following conditions apply when using these services:

- DOD Wireless Local Area Network (WLAN) Wi-Fi Connection is only authorized for Internet gateway access only due to CAC authentication limitations.
- Public Hotspot WLAN Wi-Fi Connections are not authorized.
- Home WLAN Wi-Fi Connection is protected using Advanced Encryption Standard (AES) Counter Cipher Mode with Block Chaining Message Authentication Protocol (CCMP) and therefore authorized for connection.
- The iOS Bluetooth profiles that should not be used are hands-free address book and synch profile. The STIG offers a check to verify users have not shared apps between devices. This is to protect against sensitive information being transmitted without the use of FIPS 140-2 validated encryption. (DOD, 2013)

e. iOS Browser Requirements

Safari, the iOS native browser, is disabled by MDM security policy due to CAC authentication not being support for DOD websites. Traffic will be routed through DOD Internet gateway via mobile Virtual Private Network (VPN) or the browser is installed inside the security container with a secure tunnel to the MDM server.

Mobile VPN used today to connect to DOD networks lacks the support of the CAC proxy and has issues with setup of secure connections to the back-office servers. Appendix C identifies advantages and disadvantages of the current VPN configuration. The Department of Defense is experimenting with session-based mobile VPN for secure connection to the network. Figure 3 is a notional connection illustrating this type of setup.

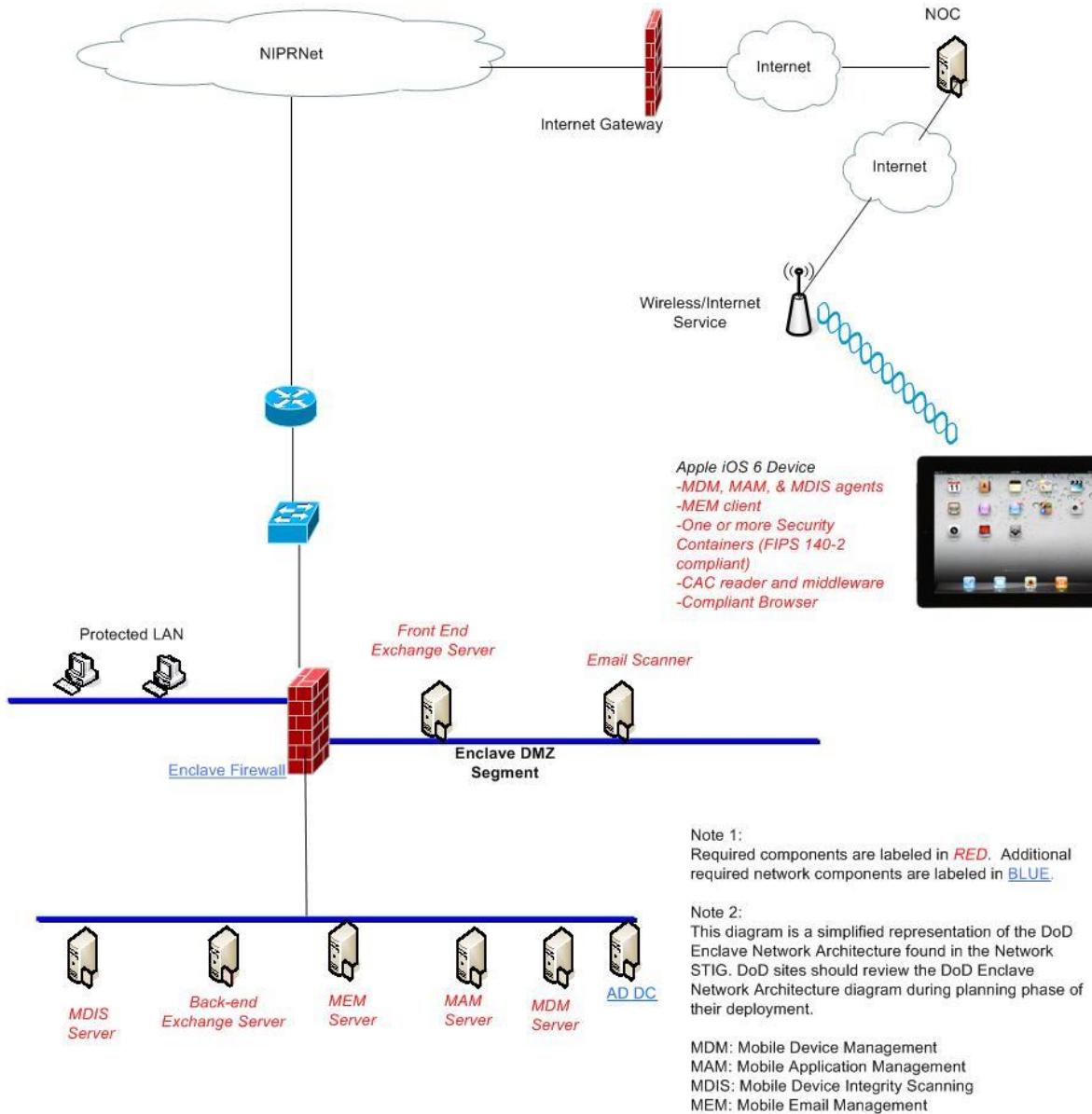


Figure 3. Notional DOD iOS 6 Connection (from DISA, 2013)

B. ACCESS CONTROL METHODS

Access control includes the process of identification, authentication and authorization for access to DOD protected information. These methods include physical, logical, and administrative controls used to protect or prevent unauthorized access to protected information. Physical controls are used to prevent access to a device interior or exterior by means of physical distance or electronic access passcode. Logical control utilizes both hardware and software in order to deter access via username and password, certificate-based authentication and/or firewalls. Administrative controls are policies, procedures, and regulations that are in place to enforce the physical and logical access controls. Physical protection is similar to the logical layered protection shown in Figure 4, necessary to gain access to an asset. However, wireless and remote access usually bypasses the physical layer of access control.

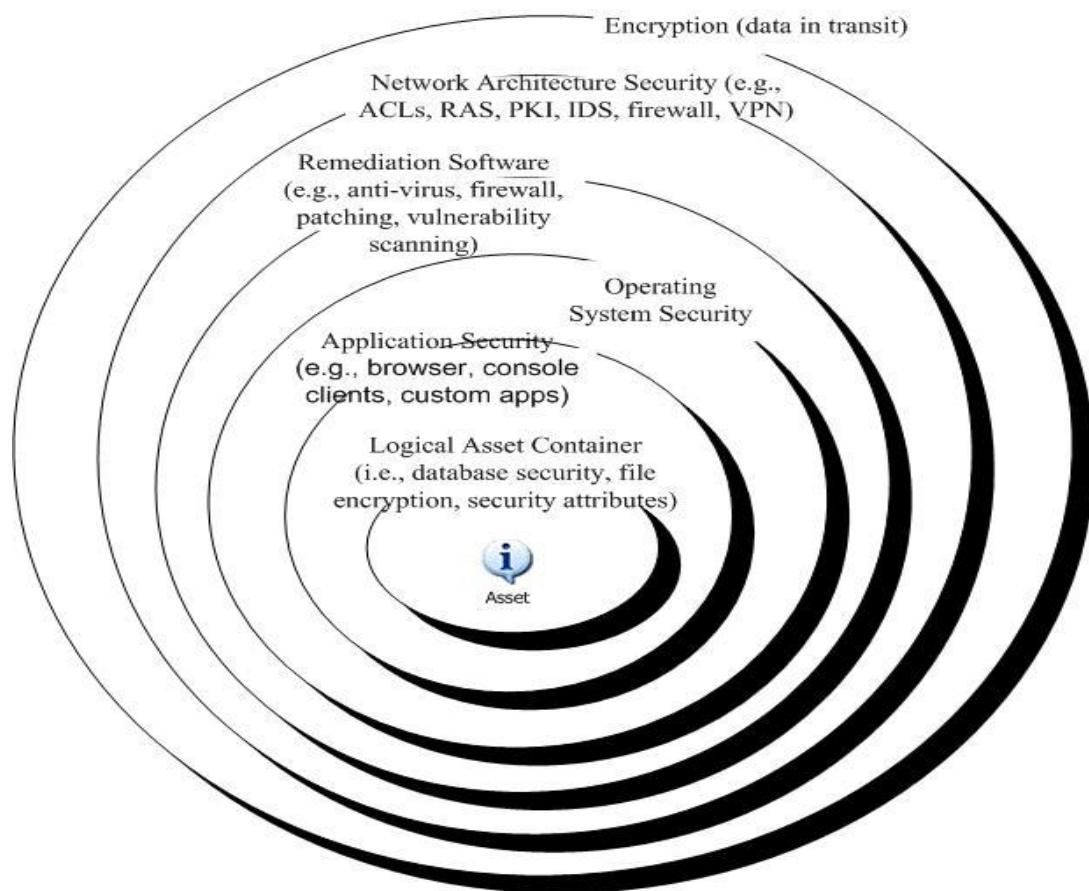


Figure 4. Layered Protection of Logical Asset (from DISA, 2010)

1. Identification Credentials

The process of identifying a user or device level of access is considered credentialing. A credential is used to validate a user or device's identity to gain access. Credentials vary depending on the level access a user or device is authorized. To gain access to a secured area one must assert an identity and provide a credential as proof of that identity (DOD, 2010).

In order to receive credential the user or device must go through the process of identity proofing. This process involves the following steps:

- Validating the claimed identity of the user or device.
- Identifier naming and registering
- Generation of an authentication credential. This can be in the form of a PIN, PKI or other identification means.
- Binding the identity to an intended authentication method.

The credential must be validated through the authentication process as part of the steps to gaining access. (DOD, 2010)

2. Authentication

Authentication the process by which a user or device credential is validated. There are three factors to validating credentials:

1. Something the user knows (e.g., a password)
2. Something the user has (e.g., CAC)
3. Something the user is (e.g., fingerprint) (DOD, 2010)

There are three levels of authentication factors: single-factor (either one of the above mention factors), two-factor (any combination of two of the above mention factors), and three-factors (a combination of all three factors). Depending on the type of technology and technique required, it is possible to use all three to achieve the highest level of assurance. Table 4 provides the various combination of assurance depending on the value of the asset being protected.

Table 4. Authentication Methods (after DOD, 2010)

| Method | Authentication Factor(s) | Description |
|----------------------------|---------------------------------|--|
| Decal | Something the user has | Decal mounted on a motorized vehicle. |
| Transponder | Something the user has | Transponder mounted on a motorized vehicle used for operating an automated entry point. |
| Badge | Something he user has | Not personalized (e.g., visit badge without name/photo). |
| Key | Something he user has | Physical key of any kind |
| Memory Card | Something the user has | Refers to memory cards without the PIN, whether personalized or not (e.g., magnetic stripe, barcode, optical or smart cards used as memory cards). |
| Smart Card | Something the user has | Refers to smart card whether personalized or not. Includes cryptographic and non-cryptographic cards. Includes all communications interface types (e.g., contact, contactless, and combi-cards). |
| | | |
| Password | Something the user knows | DOD complaint password or PIN. |
| Unshared Combination | Something the user knows | Electronic safe, cipher lock, or PIN pad combination which allows individualized PINs or combinations. |
| Shared Combination | Something the user knows | Safe, cipher lock, or PIN pad combination with shared combination. |
| | | |
| Colleague Recognition | Something the user is | Personal recognition by peers and co-workers. Considered to be attended access. Document policy and train users. |
| User Recognition | Something the user is | Attended access control implementations wherein peers or security guard/personnel perform identification and authentication. Document policy and train users. |
| Fingerprint Identification | Something the user is | Fingerprint authentication, using one-to-many match against templates or images stored in a remote database. This is not match on card. |
| Fingerprint Verification | Something the user is | Fingerprint authentication using one-to-one match against templates or images stored on the CAC biometric |

| Method | Authentication Factor(s) | Description |
|------------------------------|---|---|
| | | reference database. |
| Hand Geometry | Something the user is | Hand Geometry authentication using one-to many match against templates or images of various characteristics of the hand and finger measurements (not fingerprints) stored in a remote database. |
| Iris Scan | Something the user is | Iris Scan authentication using one-to-many match against templates or images of the eye stored in a remote database. |
| Digital | Something the user has | Issued by DOD-approved PKI. Use digital signature |
| Certificate | Something the user knows | With PIN to unlock private key |
| Cryptographic Hardware Token | Something the user has Something the user knows | FIPS 140-2 or NSA certified encryption module used in cryptographic hardware token to implement One time password device and PIN or password solution. |
| Photo ID | Something the user has Something the user is | Verified digital or optical photo ID. Use of approved procedures for verifying a non-CAC photo identification card (e.g., driver's license) |
| PIV CAC Photo | Something the user has Something the user is | Procedure for verifying the photo on the CAC. |
| PIV CAC | Something the user has | Implies that its presence and validity is verified by an automated system such as a swipe into a reader. The purpose is to validate that this a valid CAC card only. |
| | Something the user has Something that the user knows | CAC with PIN for after-hours entry into vacant workspace without after-hours attendant. |
| | Something the user has Something the user knows Something the user is | Attended or two-person access control using a CAC plus PIN. |

3. Authorization

Authorization is the process of determining if the authenticated user or device has the appropriate permits to gain access to an asset (e.g., the need to know). Every DOD-

approved public key infrastructure provides certificate-based authentication for all persons authorized access to log on to the network; however there still exists the need for mandatory/discretionary access control (DOD, 2010). In other words, authentication alone does not equal authorization to assets or security boundaries.

4. Vulnerability Category Codes

Severity category codes (CATs) are a measure of risk used to assess a facility or system security posture. Every policy identified has a severity code that is based on the realized expected loss due to a vulnerability being exploited.

Table 5. Vulnerability Severity Code Definitions (from DOD, 2010)

| | |
|---------------------|--|
| Category I | Vulnerabilities that allow an attacker immediate access into a machine, allow super-user access, or bypass a firewall. |
| Category II | Vulnerabilities that provide information that have a high potential of giving access to an intruder. |
| Category III | Vulnerabilities that provide information that potentially could lead to compromise. |

5. Logical Method

Logical methods are those techniques and technologies that are authorized for support to validate a user's identity. Although, the logical access control methods entail security techniques for network access from network architecture controls to port security, for the purpose of this thesis the focus will be on user level access security to the network; the factors for authentication.

a. Password

Prior to the advent of new technology such as PKI, username and password was used for identification and authentication in order to gain access to the network. With use of the PKI technology, it has become easier to implement multi-factor authentication requirements. This has led to the mandate to reduce the usage of password authentication authorization and require PKI authentication. This mandate authorizes the use of approved digital certificates for authentication to DOD networks, web servers, and signing/encrypting email. These certificates are primarily issued on CACs; however,

there also exist DOD approved external PKIs used to authenticate to web servers (DOD, 2010). These external certificates will not reside on the CAC; therefore, it must be kept in mind that the requirement for PKI and the CAC is simply the merger of the identification card with PKI for ease and increased assurance. This merger allows the access of multiple physical and logical assets without the need for multiple credentials and authentication tokens for access.

The CTO 06-02 states DOD is phasing out the use of passwords as a means to authenticate for the increased level of assurance the PKI certificate offers. Due to legacy systems and/or targeted audience a documented exception to policy will need to exist to utilize Alternate Login Tokens (ALT) and username and password to authenticate. This is an exception that must be approved by the service/agency PKI PMO, the DOD PKI PMO, and DAA. The policy for password configuration still stands, the requirement for length and complexity with the use of both alphanumeric and special characters.

The following are the CATs for username and password authentication:

(AC34.168: CAT III) The DAA is responsible for ensuring the use of username and password is limited to those systems that are cost prohibitive, unwarranted, and technologically not feasible. The exception must be documented and approved by the DAA, the service/agency PKI PMO as well as the DoD PKI PMO.

(AC34.170: CAT II) Information Assurance Manager (IAM) is responsible for ensuring the DoD policy for creation and change of passwords are being followed when accessing restricted areas. The must be automated procedures in place and users trained on the requirements.

(AC34.175: CAT I) Information Assurance Officer (IAO) is responsible for the removal of default passwords on install devices (e.g., databases and operating systems).

(AC34.180: CAT II) IAO is responsible for ensuring the use of individually assigned accounts for users, system, application, and database administrators.

(AC34.181: CAT II) IAO is responsible for ensuring that all shared or group authenticators for application or network access is used in conjunction with an individual authenticator. Any group authenticator not based on DoD PKI policy will be approved by the DAA.

(AC34.185: CAT II) IAO is responsible for ensuring shared/group PINs and passwords are IAW DoDI 8500.2 Auditing procedures implemented in conjunction with these methods to support nonrepudiation and accountability. (DOD, 2010)

b. Public Key Infrastructure

Public key infrastructure is a two-factor authentication process it represents something the user has and knows. When the PKI is stored on a hardware token the level of assurance is increased due to the difficulty to attack. Hardware token represents a second instance of something that you have (DOD, 2010).

The infrastructure binds the public keys and user identity by the certificate authority (CA) and the validation authority (VA) ensures that the user's identity is unique within the CA domain. The registration authority ensures that the user is bound with its public key in a way that there is non-repudiation. PKI's digital certificates when used offer the following services (DOD, 2010):

- Identification and authentication through digital signature of a challenge
- Data integrity through digital signature of the information
- Confidentiality through encryption
- Assists with technical non-repudiation through digital signatures

The PKI important component is the X.509 formatted public key. It combined with the private key produce a unique authentication. The data element includes: name of user or device; start and end date of validation; public key; name of issuing CA; and the digital signature of the CA.

The Department of Defense Instruction 8520.2 identifies requirements for PKI usage for both software and hardware. The primary token is the hardware token integrated on the CAC although there are other tokens authorized for use. Regardless of whether the PKI is utilized as a hardware or software token, in order to gain access to the private key the user is required to provide a PIN or password. The private key represents something you have and the PIN used to protect the private key represents something you know therefore providing two-factor authentication.

In order to access non-public DOD computer networks, systems, and web-based applications the use of a DOD-approved PKI certificate is required. The application must be PK-Enabled in order for a user to access it without a CAC via either an external DOD-approved PKI or a DOD compliant username/password. The PKI in itself does not grant access into a system, there is the need to have an active account and authorization.

The following is a list of access codes (ACs) and their vulnerability category for PKI utilization (DOD, 2010):

(AC34.070: CAT II) The IAM will ensure certificates are used for authentication IAW DoDI 8520.2, PKI and Public Key (PK) Enabling.

(AC34.075: CAT I) The IAM will ensure use of DoD-approved PKI digital certificates to authenticate requests for access to government information not approved for public release. For unclassified sensitive assets, the PKI certificate will be considered necessary but insufficient to provide authorized access.

(AC34.080: CAT II) The IAM will ensure implementation of certificate-based logon to the NIPRNet using DoD-approved PKI as required by DoD policy. DoD-approved PKI will be required for SIPRNet when implemented in the future.

(AC34.085: CAT I) The IAM will ensure a DoD-approved PKI certificate is used for logon to DoD Enclaves, networks, servers, desktop, laptops, and other network capable client devices. If PKI logon cannot be used, then a DoD compliant ID/password combination may be used and a migration plan implemented IAW JTF-GNO exception reporting requirements.

(AC34.090: CAT I) The IAM will ensure PKI is required for the exchange of FOUO information with vendors and contractors, the DoD will only accept PKI certificates obtained from a DoD-approved internal or external certificate authority.

(AC34.095: CAT I) The IAM will ensure DoD contractors who are not eligible for a DoD- approved PKI get and use digital certificates issued by approved external PKIs when interacting with DoD PK-Enabled information systems or accessing DoD restricted information and logical assets.

(AC34.100: CAT III) The IAM will ensure System Administrators are trained on administration and implementation of PKI and PKE. At a minimum, this training will include:

- PKI awareness training
- How to configure systems for certificate-based logon
- How to configure systems for digital signature
- How to configure systems for email encryption
- How to configure systems for Web server certificates

(AC34.105: CAT II) The IAM will require certificate-based client authentication to restricted access (not public) DoD web servers using certificates issued by DoD-approved PKI certificate authorities.

(AC34.110: CAT II) The IAO will ensure Browsers, including those that support software tokens, support the use of DoD-approved PKI, High Assurance Remote Access (HARA) solution (as appropriate for the classification level), or NSA certified solution for storing the user's certificates. (DOD, 2010)

c. DOD Common Access Card

The CAC is the approved hardware token for DOD. There are other hardware tokens available for use however they do not offer the same increased level of assurance. The CAC is the integrated solution for both identification and access control. It is the merging of the user's personal identification with the PKI certificate and keys.

Figure 5, according to DOD (2010), is an illustration without being an exact representation of the layout of the CAC. This illustration highlights the purpose of its components and technologies discussed herein. The CAC currently has many demographic data elements stored in its integrated circuit chip (ICC). Most of these elements are also printed on the card. A cryptographic co-processor and secure storage supports the DOD-approved PKI functionality. The complexity of the microprocessor is the primary distinguishing feature between a smart card and a memory card. The CAC's barcodes and magnetic stripe store data that can be used by various DOD applications, thus, the CAC can also be used as a memory card. The magnetic stripe has no data encoded on it at issuance. Organizations may use standard magnetic stripe technology to write data to the magnetic stripe. Most applications using the ICC will use the CAC to establish user authentication and trusted communication channels, but application data will reside in remote databases.

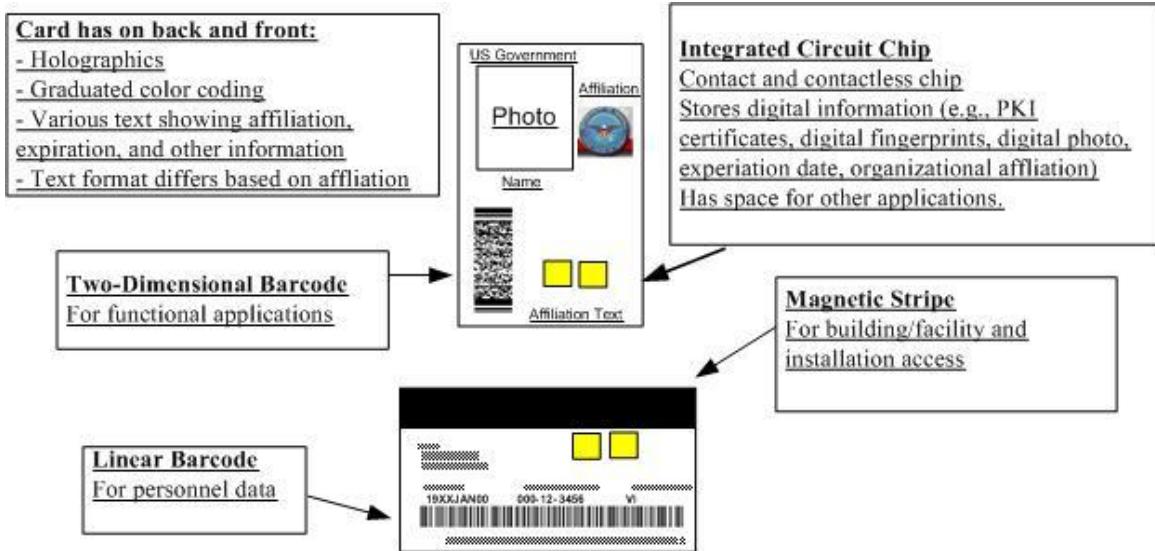


Figure 5. General Illustration of CAC Layout (from DOD, n.d.)

The biometric data being stored on the personal identity verification (PIV) version of the CAC will increase the level of assurance by representing all three factors of authentication. Through the use of the photograph and fingerprinting (something the user is), PIN (something the user knows) and CAC (something the user has) making the PIV the highest level of assurance that can be achieved.

d. The Process of the Biometric System

Biometrics are becoming more and more prevalent as technology is advancing in order to address the issue with identity theft, computer fraud, and unauthorized access to name a few. Companies are developing many methods for biometric use as technology advances and the demand increases.

The DOD is planning for the use of a central biometric repository, which will support biometric technology for both battlefield applications, as well as support services. Biometric authentication is often used to enhance security. However there are inherent risks associated with its use alone. When biometric data is compromised it is not like a compromised password or a lost/stolen CAC; it cannot just be changed or replaced. Therefore, DOD requires it to be combined with another form of authentication such as a password or PIN IAW DOD-approved PKI policy.

Biometrics can serve as either an identification or verification process. The identification process is a more complicated process in that it is a one-to-many, taking the known profile and comparing it against many to get a possible match. Whereas verification is a one-to-one process, where a user simply takes the known profile and compares it against a stored profile for a user to validate a match.

6. Enrollment into the Biometric System

Enrollment requires some form of verification other than biometric to prove a user one is the one who he or she claims to be. The stronger the initial identity verification the less likely an imposter will be able to impersonate in order to authenticate. The enrollment after the initial verification is a process that is implemented in the following stages: capture, extraction, package creation and assurance, and package storage.

In the Capture stage, biometric technology is used to record a user's physical characteristic or behavior. The hardware performing the reading is called the *capture device*. Capture devices typically are designed to capture one biometric characteristic such as a fingerprint, retina pattern, or keyboard dynamic.

In the Extraction stage, the captured information from the capture device is translated into a digital representation of the biometric characteristic. This digital representation is known as the *biometric template*.

In the Package Creation and Assurance stage, the biometric template is associated or bound with the user's identity information (e.g., name, ID, etc.). The package is then encrypted and digitally signed to protect its integrity and confidentiality.

In the Package Storage stage, the biometric package is encrypted and signed package is written to a non-volatile storage medium for future use in the verification process. This storage medium may, or may not, be integrated into the biometric system. For example, packages might be transferred to a smart card or external database. (DOD, 2010)

a. Verification of the Biometric System

According to DOD (2010), the stages of the verification process include Identification, Capture, Extraction, Package Retrieval and Validation, and Comparison. These stages are detailed below.

Identification—requires the user to present some form of ID for verification purpose.

Capture—the same process identified for enrollment.

Extraction—the same process as biometric template identified during enrollment however it's called live sample.

Package Retrieval and Validation—the biometric package is retrieved from storage and decrypted. Its digital signature is validated to ensure that it was created during the enrollment process and not modified since then.

Comparison—The live sample and biometric template are provided as inputs to a software module known as the comparator, which generates a score describing how close a match the two are to one another. Based on predetermined thresholds, the two are either declared a match given the

resulting score (*acceptance*) or they are not (*rejection*). The determination is forwarded to whatever access control system the biometric technology is supporting. (DOD, 2010)

b. Separation of Duties in the Biometric System

Administrators are the only users to interact with the system beyond the biometric capture device. Therefore, improper administrative access has the potential to cause extreme risk to the system. The administrators for the system will need to authenticate to the biometric software before any access to controls can be granted. This is an alternate authentication in the event that the system has been compromised or is not functioning properly.

According to DOD (2010), as specified by *Biometric Verification Mode Protection Profile for Medium Assurance Environments*, the duties of the administrative function should be separate due to the three identified roles in order to prevent a conflict of interest as well as for check and balance.

- Enrollment Administrator—is responsible for verifying the identity of new users and walking them through the process of enrollment.
- Security Administrator—is responsible for establishing and updating/modifying the configuration parameter values of the software.
- Audit Administrator—is responsible for reviewing audit logs for security violations and related suspicious behavior.

The combination of any or all of these roles can pose an extremely adverse integrity issue that could potentially allow the administrator to tamper with the system in such a way as to make it easy to breach. Whether the software allows for separation of these roles or not the information assurance officer should ensure that there are measures in place to mitigate this risk. The following are biometric codes that and their categorical vulnerability levels:

(BIO1010: CAT II) The IAO will ensure individuals are assigned in writing to the following administrative roles: Enrollment Administrator (enroll or re-enroll users); Security Administrator (modify the security configuration), and Audit Administrator (review and manage audit logs).

(BIO1020: CAT II) The IAO will ensure the following functions are restricted to authorized Administrators:

- Creation or modification of authentication and authorization rules
- Creation, installation, modification or revocation of cryptographic keys
- Startup and shutdown of the biometric service

(BIO1030: CAT II) The IAO will ensure only authorized Enrollment Administrators are permitted to create user biometric templates.

(BIO1040: CAT III) The IAO will ensure only authorized Audit Administrators can clear the audit log or modify any of its entries.

(BIO1050: CAT II) The IAO will ensure all Administrators must authenticate to the biometric system to perform administrative functions and that this authentication must include a factor outside of the biometric verification the system supports for ordinary users. (DOD, 2010)

Figure 6 is a depiction of the various levels of logical access control that are authorized for use within DOD for verification and validation of the identity of a user.

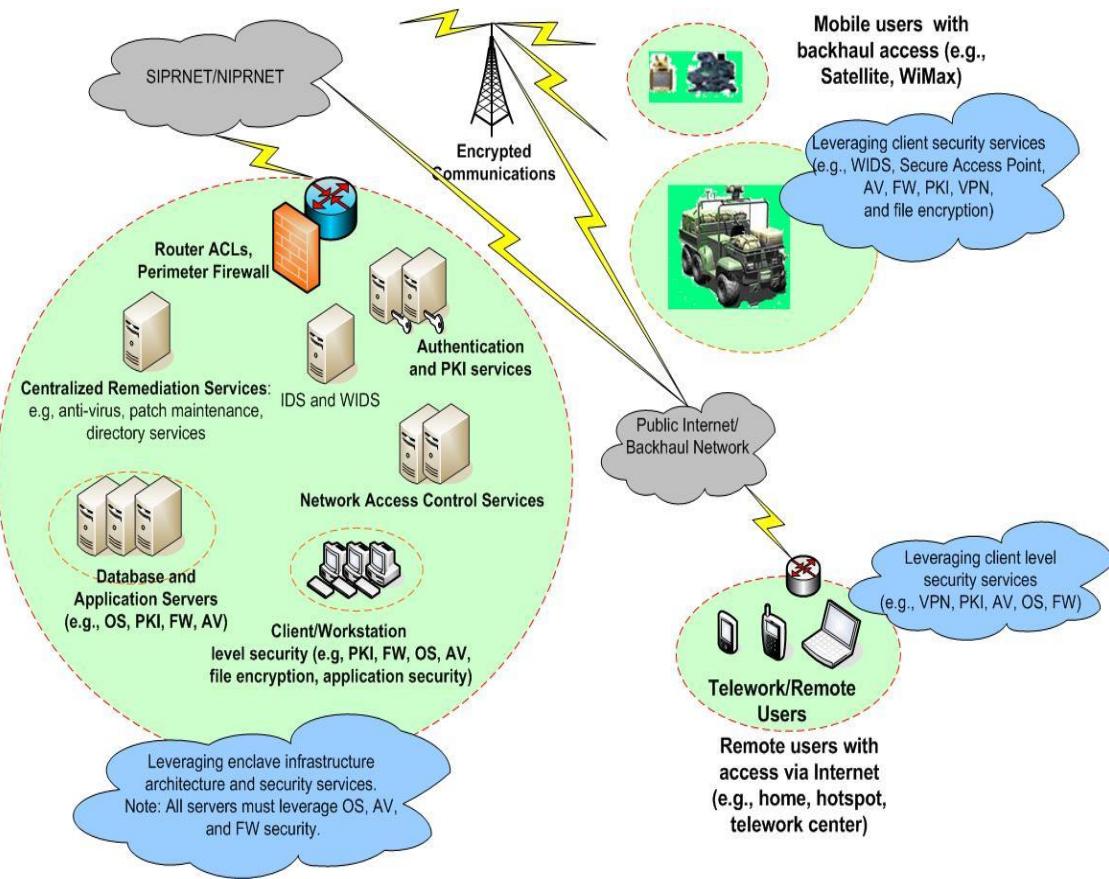


Figure 6. Notional Example of Leveraging Logical Security Services (from DISA, 2010)

THIS PAGE INTENTIONALLY LEFT BLANK

IV. TESTING AND EVALUATION

In the past decades, mobile devices have significantly changed business capabilities, allowing employees access to information resources wherever they are, whenever they need to (NIST, 2014). Technologies have allowed access to otherwise protected information wherever and whenever creating both opportunities and challenges. Due to this ever-growing demand to use personal mobile devices DOD has had to establish security policies, which have been outlined in the previous chapters. This chapter will demonstrate and analyze the ways and challenges associated with securely access a Department of the Navy (DON) website in order to launch training. Due to circumstances outside of our control we were only able to test iOS device. The Android, along with a more comprehensive testing of the VDI, will be identified for follow-on research.

A. TESTING SCENARIOS

The purpose of the demonstrations is a proof of concept that you can actually access, enroll, and launch training via a personal mobile device. These examples will demonstrate that with the proper technologies and adhering to the proper security measures, one can use their personal mobile device to conduct training whenever and wherever.

1. iOS and PKard Smart Card Readers

Thursby is the company that produces the PKard CAC reader for iOS devices, which includes iPhone 4S or later, iPad 2Gen or later, and iPad mini. There are two form factors for the readers as pictured in Figure 7.



Figure 7. Plug-in and Case CAC Readers or the iOS (from thursby.com)

The items necessary to make the connection to NeL are either of the mentioned mobile devices, PKard reader, CAC, and Internet connection. Both the Plug-in and the Case as well as the iPhone, iPad, and iPad mini were used for the purposes of the demonstration and all yield the same results. The reader once connected to the mobile devices prompts the user to download the associated application necessary to use the reader¹. The following are the steps used via all the iOS devices to gain access, enroll, and launch training on the NeL site. Once the application is loaded Figure 8 appears.

¹ See
http://www.thursby.com/sites/default/files/images/iPad%20and%20iPad%20Mini%20PKard%20Reader_3.pdf and
http://www.thursby.com/sites/default/files/images/iPad%20iPhone%20iPod%20PKard%20Reader_2.pdf
for the specifications and features of the card readers

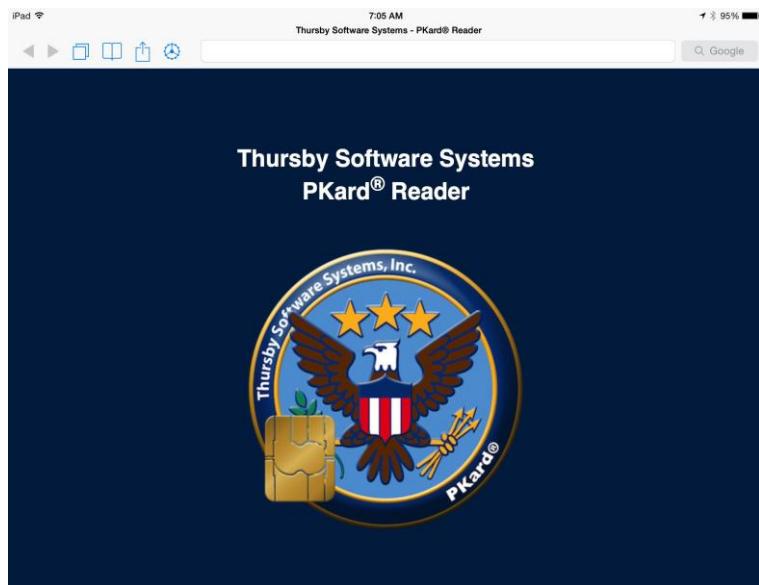


Figure 8. Screen Capture of the Application Used for the PKard Reader

Next, the user will be asked to select the sites he or she wishes to import for easy use of access. This step preloads all the DOD sites that require CAC in order to access. This import is shown in Figures 9 and 10 as bookmarks.



Figure 9. Screen Capture of the Import of DOD Sites

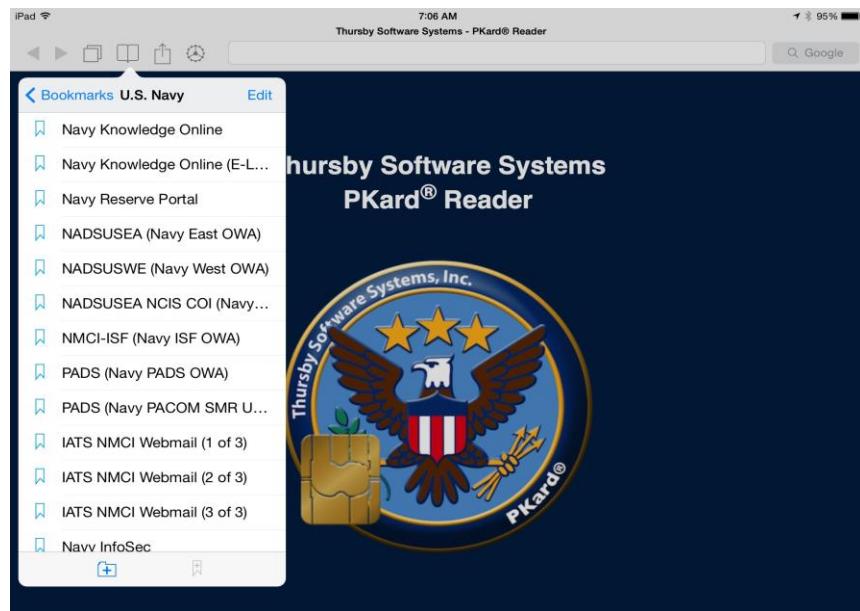


Figure 10. Screen Capture of the U.S. Navy Sites

After importing the sites to bookmark, the user then can click on a folder that will take her or him to the list of available site. Navy Knowledge Online (NKO) was used for this purpose in order to get to NeL site. This is illustrated in Figure 11.

The arrow points to the symbol that indicates that the CAC has been inserted into the reader and the reader is retrieving the certificates from the CAC. The certificates are the ones that will be shown in Figure 12. Once the reader has retrieved the certificates, the symbol will reflect a frame with a card inserted as shown in Figure 13.

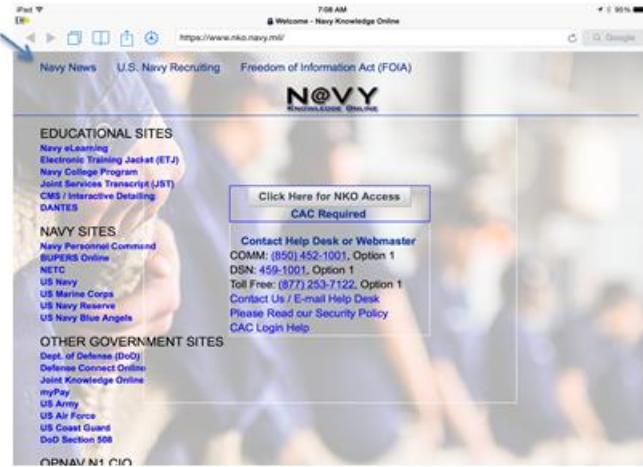


Figure 11. Screen Capture of NKO Site

Once on the NKO site, the user clicks the Navy e-Learning link and will be redirected to a page to select the appropriate client certificate as shown in Figure 12.

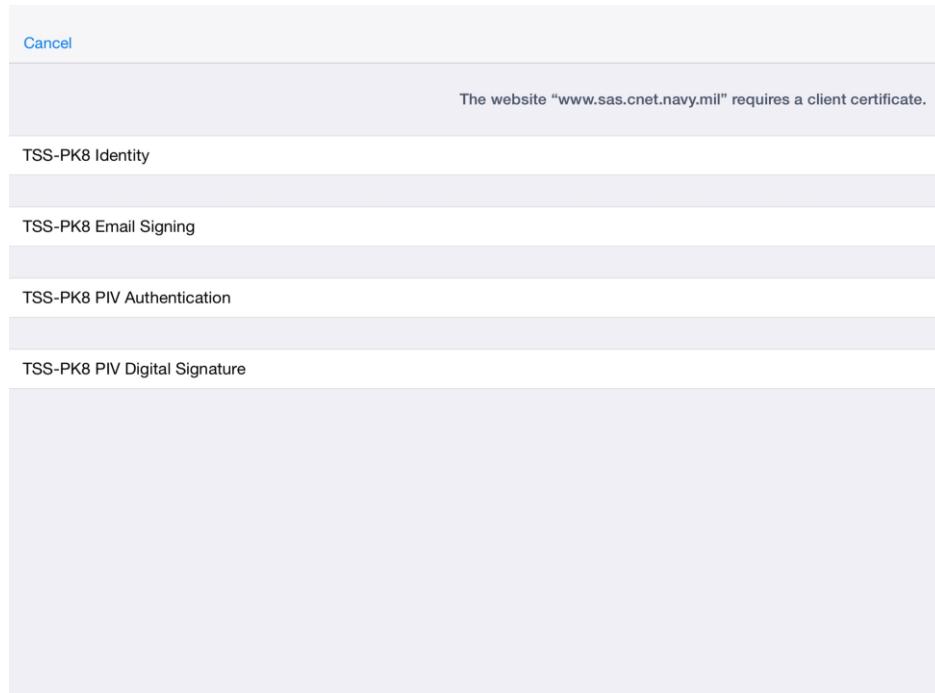


Figure 12. Screen Capture of Client Certificates

Next, the user will be prompt to enter his or her PIN this is the six digit numeral code associated with the user's CAC for the two factor authentication process for PKI. This is shown in Figure 13.

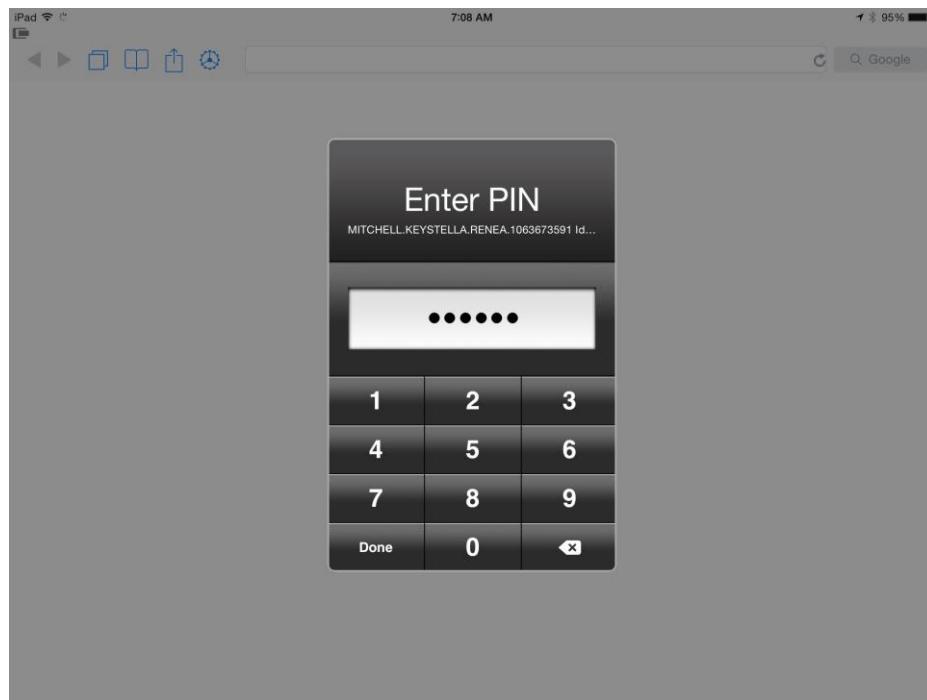


Figure 13. Screen Capture of Authentication Request

Once the handshake is made and the authentication process is complete the user is then granted access to the site as shown in Figure 14.

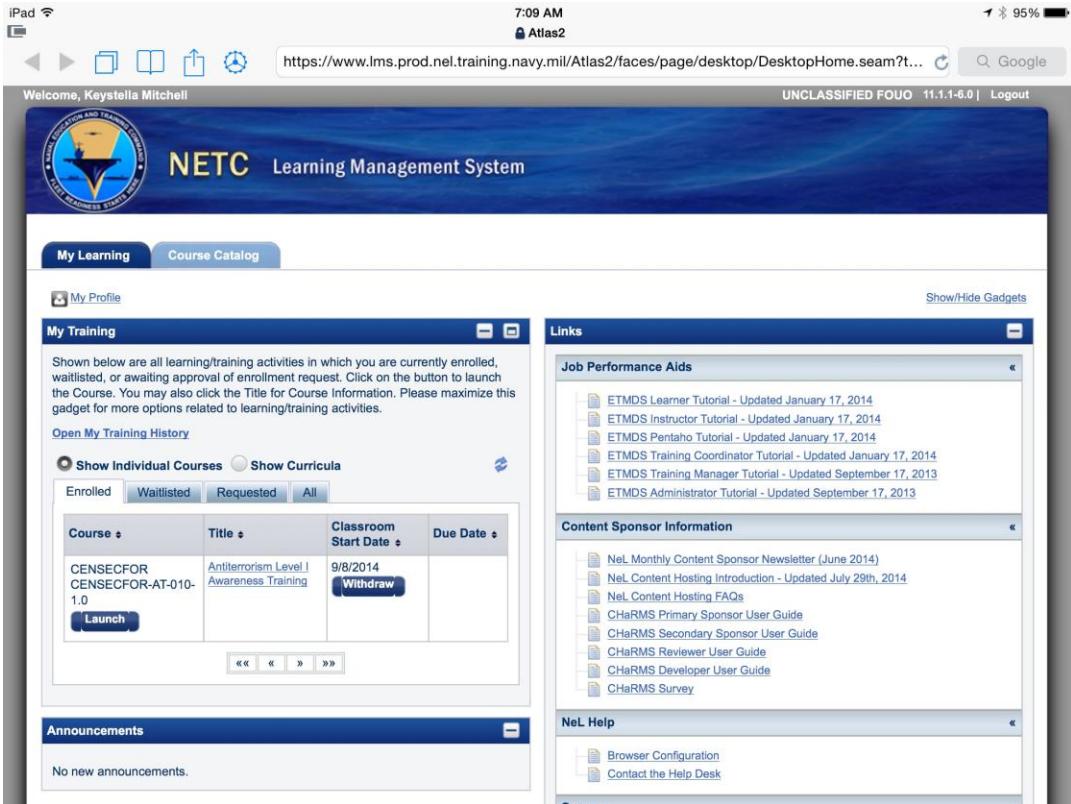


Figure 14. Screen Capture of NETC Learning Management System site

Once the user has successfully access the NeL site, she or he is able to perform the same functions as if she or he were using a desktop or laptop device. Functions such as enrolling in a course browse the site as will be depicted in the following Figures 15–17.

The screenshot shows the Course Catalog page of the NETC LMS site. At the top, there are tabs for 'My Learning' and 'Course Catalog'. Below them are 'My Profile' and 'Courses' tabs. A search bar at the top right contains the text 'Google'. The main content area is titled 'Browse Course Catalog' and includes a 'Learning Category' section with a grid of course links. Below this is a table of courses with columns for Prefix, Number (suffix), Title, and Course Status. Each row has an 'Enroll' button and a green plus sign icon.

| Prefix | Number (suffix) | Title | Course Status |
|------------|-------------------|--|-------------------------|
| CENSEALSWC | CENSEALSWC-NSW-02 | Naval Special Warfare (NSW) Communication Capabilities | <button>Enroll</button> |
| CENSECFOR | CANS-AS1-IT21-1.0 | Armed Sentry Duties Part I (IT21) | <button>Enroll</button> |
| CENSECFOR | CANS-AS1-NMCI-1.0 | Armed Sentry Duties Part I (NMCI) | <button>Enroll</button> |
| CENSECFOR | CANS-AS2-IT21-1.0 | Armed Sentry Duties Part II (IT21) | <button>Enroll</button> |

Figure 15. Screen Capture of Course Catalog NETC LMS site

This screenshot shows a modal dialog box titled 'Course Enrollment - CENSECFORCSF-PFS-010'. It asks the user if they want to enroll in the course 'CENSECFORCSF-PFS-010 -Personal Firearm Safety?'. There are 'Continue' and 'Cancel' buttons at the bottom of the dialog. The background shows the same course catalog interface as Figure 15.

Figure 16. Screen Capture of Enrollment into a Course NETC LMS site



Figure 17. Screen Capture of Confirmed Enrollment on NETC LMS site

The process to gain access and enroll is the same regardless of the type of PKard reader and iOS device used. It is a very straightforward process. The test was to actually launch training. After gaining access and being able to enroll that seemed to be a relatively simple task to accomplish; however, upon attempting to launch a training session it was unsuccessful. This was due to the language the training is written in. The native browser for iOS, Safari, does not support Flash, which is what naval training is developed in.

a. Attempts to Launch Training

Several attempts were made to do a work around to get the training to launch. There was an attempt to use an application browser that supported Flash; however, because the Thursby Software System was developed strictly to support the native browser there was no way to launch another browser application and then invoke the Thursby Software system on top or vice versa.

There was an attempt to use a virtual machine (VM) to access NeL in order to use a browser that would support Flash. In this experiment, we set up a standalone VM environment to see if we could use the flash-supported browser in the VM to launch a lesson remotely from an iOS device using the Horizon VM View client². We were able to access the VM and invoke a web browser with username/password authentication from an iOS device. However, when accessing the VM remotely with the user's CAC credential via the Horizon VM View client and the PKcard reader, we got a blank screen instead of the remote desktop.

2. iOS and baiMobile Smart Card Reader

Biometric is the company that produces the baiMobile CAC reader for iOS devices, which include iPhone 4S or later, iPad 2Gen or later, and iPad mini. There are two form factors for the readers as pictured below in Figures 18 and 19.



Figure 18. 3000 MP Bluetooth Smart Card Reader (from biometricassociates.com)

² See <http://www.vmware.com/pdf/horizon-view/horizon-client-ios-document.pdf> for details.



Figure 19. 301MP LT Smart Card Reader (from biometricassociates.com)

The required items necessary for the reader to work are the mobile device, baiMobile reader, CAC, and Internet connection. The baiMobile 301MP LT was used for the purposes of this demonstration³. The initial setup started similar to the PKard with the connection and prompt to download the associated applications; however, that is where the similarities ended. The baiMobile reader requires the use of the baiMobile Credential Service application, which is third party software that requires the user to establish an account with the Biometric Associates, and store the user's certificates on their server. There was no attempt made to connect via this means because the intent is to be able to connect without having to deal with an entity in the middle. Moreover, we were not able to log onto NeL directly using either the Horizon VM View Client or the Receiver VM View Client and the baiMobile reader.

The 3000 MP Bluetooth Reader is another biaMobile device that makes the claims that it supports DOD CACs and through the use of the reader and middleware access to credentials is made available to support such functions as digital signing and decrypting emails, and authenticating to secure websites and network servers. The software that supports the reader is currently offline due to updates being made by the Biometric Associates.

³ The specification for both readers can be found in <https://www.biometricassociates.com/products/smart-card-readers/301mp-reader/> and <https://www.biometricassociates.com/products/smart-card-readers/3000mp-reader/>.

B. EVALUATION OF TESTING

The following research questions were addressed: 1) Can a secure connection via a mobile device be made to access NeL site? 2) Is enrollment into a training session via a mobile device possible? 3) Can a training session be launched and completed via a mobile device? A secure connection can be achieved via a mobile device to the NeL site. This was made possible by the PKard reader (one of two CAC readers tested) as illustrated in Scenario 1 Figure 14. This is significant because it is the first and most important step to establishing training whenever and wherever.

The establishment of a connection to CAC enabled DOD networks via a personal mobile device opens the door to many more possibilities of use on a protected unclassified network. This could potentially free up space on networks and reduce the cost of maintenance for IT devices. This testing can serve as another view of BYOD and its possibilities.

Enrollment into a training session was possible. Once connection was made the functionality of enrollment was the same as it would be if we were using a desktop or laptop. We are able to select the type of display we would prefer and the appearance is similar.

The ability to launch and complete a training session was not as successful as expected. We are prompt to launch a session; however, upon doing so with iOS devices we are directed to a blank screen because of the incompatibility of the native browser and the language in which the training is developed. This is due to DOD primarily supporting Windows Internet Explorer and Flash.

Overall, the testing was a success with the establishment of a secure connection, enrollment into a training session and the ability to access and other sites that proved that given training being developed in a language that is support by all browsers then one could successfully launch and complete a training session.

We were not able to test the Android devices due to end of year contracting constrains. Table 6 illustrates the devices and methods used as well as the ability to gain access to a CAC enabled website.

Table 6. Test Matrixes for NeL Site

| | iPhone & iPad | | | | Android Phones & Tablets | | | |
|-------------------|---------------|--------------|------------------|--------------------|--------------------------|--------------|------------------|--------------------|
| Mobile Device OS | iOS 7 | PKard Reader | baiMobile Reader | Derived Credential | Android 4 | PKard Reader | baiMobile Reader | Derived Credential |
| Secure Connection | Y | Y | N | N/A | N/A | N/A | N/A | N/A |
| VM Authentication | | N | N | N/A | N/A | N/A | N/A | N/A |
| Enrollment | | Y | N | N/A | N/A | N/A | N/A | N/A |
| Training | | N | N | N/A | N/A | N/A | N/A | N/A |

Y= Yes N= No N/A= Not Tested

The testing proved to be successful for the purpose of this thesis because access was granted, enrollment was established, and training was attempted from an iOS with a PKcard smart card reader. The necessary security requirements are in place to establish a connection in order to conduct training. Although, some will insist that it is only a partial success because training was not accomplished we would argue that is an issue that requires not just the DoN but also the DOD to support more than just one browser type if the intent is to make information access whenever and wherever. That means developing information that is supported by such languages as HyperText Markup Language or JavaScript. This is something that can be achieved; the Defense Travel System (DTS) has managed to crack the code on this. Defense Travel System was one of the many DOD sites that were accessed in our attempts to evaluate the possibility of accessing secured DOD sites using mobile devices. Once we authenticated with the DTS site using the PKard reader and software, we were able to create a travel request as well as a voucher request via Safari browser. We were also able to access Marine Online (MOL) and create a leave request using an iOS device with the PKard smart card reader.

The results of the testing indicates that with any IT solution there are issues to overcome either in the form of training or performance. Both were experienced during these testing. There is a need for a quick reference or guide to explain the setup of the CAC reader with each mobile device it supports.

There are some definite drawbacks such as cost of the reader, form factor, the use of VMware, and updates to the operating system (OS). The reader regardless of the

developer or the type of device it supports runs from \$100.00 to \$350.00. The form factor is a potential drawback for those plug-in readers. The VMware must be setup to support CAC in order to make the secure connection. Due to continuous updates to the OS and the requirement for middleware there exist the potential for incapability between the mobile device and the reader.

V. CONCLUSION AND FUTURE RESEARCH

A. CONCLUSION

This thesis demonstrated the ability to establish a secure connection to a DOD CAC enabled site via a personal mobile device given the current security policies and technologies. Once the two-factor authentication was accepted, we were able to enroll in a training course. However, due to browser incompatibility, we were not able to launch and complete training via the personal mobile device.

The ability to establish and maintain a secure connection via a personal mobile device will open the door to many other opportunities that can prove to be cost effective and beneficial for DOD. There is a need for future research to be done in this area because it is just another capability of BYOD that has the potential to extend the DOD network.

B. FUTURE RESEARCH

There are many areas of future research that stem from this thesis that will assist in informing DON of the right approach to take in moving closer to a BYOD strategy. We have provided some examples of these areas of research below.

1. Continued Testing of Approved Mobile Devices and Methods

Due to time constraints and inability to test all devices and methods there exist the need to continue testing the iOS and initiate testing of the Android devices for access and compatibility.

2. Support of Multiple Browsers

In light of the incompatibility issues with native browsers on various mobile devices it would be beneficial to do the necessary research to look into what would be needed to train in a language that is supported by all browsers such as HTML.

3. Support of CAC Enable Sites via VMWare

The use of a VM adds an additional layer of secure to using mobile devices. The VM gives added assurance that once the connection is lost no information will reside on the device. This helps to make mobile computing more acceptable.

4. Support of Soft Certification

The ability to access a CAC enabled site via a soft certification is a capability that is desperately needed as technology continues to improve. The form factors of CAC readers are more cumbersome than the mobile device itself. There are definitely better and just as secure ways to access credentials for a mobile device instead of a hardware only solution. It is potentially more cost effective and efficient as well.

5. Classification of Information

This may seem unrelated to this thesis. However it makes all the difference in how information is handled. There needs to be an in-depth review of policy on what, how, and why information is classified the way it is. This could potentially take the strain of trying to protect information that is already public knowledge due to the great world of the Internet.

6. Hosting a .Com Site

This would go hand in hand with classification of information research: Is there a need for all information pertaining to the DOD to reside in the .mil domain? What would be the potential benefits of establishing such a domain to give access to information that does not require protection and pose no threat to national security accessed by the adversary?

C. SUMMARY

This thesis has been informative to the various technologies that exist today that support secure connection of mobile devices to a DOD network. It also demonstrates the strides DOD is making to partner with industry in order to keep pace with technology.

The Department of Defense is not there yet and understandably so due to the need to maintain national security with such initiatives as the *Mobile Device Strategy* it is well on its way. The items identified for future research could help to close that gap.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. SAMSUNG ANDROID WITH KNOX 1.X V2R1 OVERVIEW

The following is an excerpt from the *Samsung Android (with Knox 1.x) Security Technical Implementation Guide (STIG) Overview V2R1*. The table shows sample configurations for the deployment of Knox containers (Samsung & Defense Information Systems Agency, 2014b, p. 12).

UNCLASSIFIED

3.11 Recommended Container Configuration

The following table shows a sample configuration for enterprises deploying Knox containers. This is provided to show options available to enterprises to further lock down the Knox container for work use. Even though Knox container management policies are available from several MDM vendors, availability of individual policies may differ for each vendor.

| Policy | Setting | Description |
|----------------------------------|-------------------------------------|--|
| Application Whitelist | Enterprise whitelist of application | Only those applications on the whitelist can be installed from the Knox Application store. |
| Minimum password length | 6 | Container password must be 6 characters or more. |
| Password quality | Alphanumeric | Password must contain letters and numbers. |
| Maximum time to lock | 15 | Container will auto-lock after 15 minutes of inactivity. |
| Minimum character change length | 2 | User must change at least 2 characters when changing the password. |
| Maximum failed password attempts | 10 | Container will be admin locked when the user fails to enter the correct password on 10 attempts. |
| Set HTTP proxy | DoD proxy address | All browser traffic will be directed to the DoD proxy server. |
| Account whitelist | Enterprise email address domain | Only enterprise email accounts will be allowed inside the container. |
| Browser smartcard authentication | Enable | Enables smartcard authentication (using the Bluetooth CAC reader) for the browser. |
| Email smartcard credentials | Enable/DoD email account | Enables smartcard credentials (using the Bluetooth CAC reader) for the specified email account. |

APPENDIX B. SAMSUNG ANDROID WITH KNOX 1.X V2R1 CONFIGURATION TABLE

UNCLASSIFIED



SAMSUNG ANDROID (with Knox 1.x) STIG CONFIGURATION TABLE

Version 2, Release 1

17 April 2014

Developed by Samsung and DISA for the DoD

UNCLASSIFIED

UNCLASSIFIED

Samsung Android (with Knox 1.x) Configuration Table, V2R1
17 April 2014

DISA Field Security Operations
Developed by Samsung and DISA for the DoD

This page is intentionally left blank.

ii

UNCLASSIFIED

UNCLASSIFIED

Samsung Android (with Knox 1.x) Configuration Table, V2R1
17 April 2014

DISA Field Security Operations
Developed by Samsung and DISA for the DoD

| Policy Group | Policy Rule | Options | Required | Optional | Settings | Related Requirement Number | Comments |
|---------------------|----------------------------------|------------------|----------|----------|------------------------------|----------------------------------|--|
| Android Restriction | Storage Encryption | Enable / Disable | X | | Enable | KNOX-20-004400 | Encrypt all user and enterprise data at rest. |
| Android Restriction | External Storage Encryption | Enable / Disable | X | | Enable | KNOX-20-004400 | Encrypt all external media cards. |
| Android Restriction | Disable Camera | Enable / Disable | | X | Enable | | |
| Android Restriction | Disable Microphone | Enable / Disable | | X | Enable | | |
| Android Restriction | Disable WiFi Tethering | Enable / Disable | | X | Enable | | |
| Android Restriction | Disable Developer Mode | Enable / Disable | X | | Disable | KNOX-25-009300 | |
| Android Restriction | Disable Location | Enable / Disable | | X | Enable | | |
| Android Restriction | Disable USB Debugging | Enable / Disable | X | | Enable | KNOX-25-015800 | |
| Android Restriction | Allow Mock Locations | Enable / Disable | X | | Disable | KNOX-25-015900 | |
| Android Restriction | Disable USB Media Player | Enable / Disable | X | | Enable | KNOX-25-009800 | |
| Android Restriction | Disable Vendor USB Protocol | Enable / Disable | X | | Enable | KNOX-23-013700 | |
| Android Restriction | Disable Manual Date Time Changes | Enable / Disable | X | | Enable | KNOX-28-012600 | |
| Android Restriction | Bluetooth Whitelist | Configure | X | | Add Bluetooth Manufacture ID | KNOX-23-012700 KNOX-23-013100 | Restricts Bluetooth devices allowed to pair with the device. |

1

UNCLASSIFIED

UNCLASSIFIED

Samsung Android (with Knox 1.x) Configuration Table, V2R1
17 April 2014

DISA Field Security Operations
Developed by Samsung and DISA for the DoD

| Policy Group | Policy Rule | Options | Required | Optional | Settings | Related Requirement Number | Comments |
|------------------------------|-------------------------------------|------------------|----------|----------|-------------------|----------------------------|---|
| Android Restrictions | Allowed Bluetooth Profiles | | X | | HFP HSP SPP | KNOX-29-015700 | Disables all Bluetooth profiles except for those specified in the settings. |
| Android Restriction | Disable Insecure VPN Connections | Enable / Disable | X | | Enable | KNOX-23-012800 | |
| Android Restriction | Web Proxy | Configure | X | | Add Web Proxy | KNOX-23-013400 | IP address and port of the DoD proxy. |
| Android Restriction | Allow cookies | Enable / Disable | | X | | | Native browser application only. |
| Android Restriction | Enable auto-fill | Enable / Disable | | X | | | Native browser application only. |
| Android Restriction | Enable JavaScript | Enable / Disable | | X | | | Native browser application only. |
| Android Restriction | Enable popups | Enable / Disable | | X | | | Native browser application only. |
| Android Restriction | Enable CAC authentication for email | Enable / Disable | | X | | | For native email client. |
| Android Restriction | Enable Google Play | Enable / Disable | X | | Disable | KNOX-25-009000 | |
| Android Restriction | Allow Unknown Sources | Enable / Disable | X | | Disable | KNOX-25-009000 | |
| Android Advanced Restriction | Enable CC Mode | Enable / Disable | X | | Enable | KNOX-29-015600 | Puts the devices in (Common Criteria) CC Mode as defined by the Samsung Galaxy Device MDFPP Security Target. If the configuration is not |

UNCLASSIFIED

Samsung Android (with Knox 1.x) Configuration Table, V2R1
17 April 2014

DISA Field Security Operations
Developed by Samsung and DISA for the DoD

| Policy Group | Policy Rule | Options | Required | Optional | Settings | Related Requirement Number | Comments |
|----------------------|---------------------------------------|------------------------|----------|----------|------------------------|----------------------------|---|
| | | | | | | | available on the MDM console, install the Samsung CC Mode Android Application Package File (APK) and enable CC Mode. The APK is available on Google Play. |
| Android Restriction | Enable CAC authentication for browser | Enable / Disable | | X | | | Native browser application only. |
| Android Restriction | DoD Banner | Enable / Disable | X | | Enable | KNOX-26-009700 | |
| Android Firewall | Firewall | Configure | X | | Add IP address / Ports | KNOX-23-012900 | |
| Android VPN | VPN | Configure | | X | Add VPN Profile | | Configure organization VPN profile. |
| Android Certificate | Certificate | Configure | X | | Add Certificates | KNOX-22-013200 | Select PEM-encoded representations of the DoD root and intermediate certificates. |
| Password Restriction | Maximum Failed Attempts | 0- | X | | 10 | KNOX-24-008900 | Unsuccessful login attempts before device wipe. |
| Password Restriction | Minimum Length | 0- | X | | 6 | KNOX-24-008700 | Minimum device password length. |
| Password Restriction | Password Complexity | Pattern Pin Alphabetic | | X | | | Device password complexity. |

UNCLASSIFIED

Samsung Android (with Knox 1.x) Configuration Table, V2R1
17 April 2014

DISA Field Security Operations
Developed by Samsung and DISA for the DoD

| Policy Group | Policy Rule | Options | Required | Optional | Settings | Related Requirement Number | Comments |
|----------------------|---------------------------|----------------------|----------|----------|-----------------------|----------------------------|--|
| | | Alphanumeric Complex | | | | | |
| Password Restriction | Maximum Password Lifetime | 0- | | X | | | Days after which password must be changed. |
| Password Restriction | Max Time to Lock | 0- | | X | 15 | KNOX-24-008800 | Minutes of inactivity after which device will lock. |
| Password Restriction | Min Uppercase | 0- | | X | | | Minimum number of uppercase alphabetic characters in device password. |
| Password Restriction | Min Lowercase | 0- | | X | | | Minimum number of lowercase alphabetic characters in device password. |
| Password Restriction | Min Numeric | 0- | | X | | | Minimum number of numeric characters in device password. |
| Password Restriction | Min Mutation on Change | 0- | | X | | | Minimum number of characters that must be changed when device password is changed. |
| Password Restriction | Max Sequential Characters | 0- | | X | | | Maximum number of sequential characters in device password. |
| Application | Application White List | Configure | X | | Add Approved Packages | KNOX-25-009100 | |
| Application | Application Black | Configure | | X | Add Packages | | |

UNCLASSIFIED

Samsung Android (with Knox 1.x) Configuration Table, V2R1
17 April 2014

DISA Field Security Operations
Developed by Samsung and DISA for the DoD

| Policy Group | Policy Rule | Options | Required | Optional | Settings | Related Requirement Number | Comments |
|--------------------------------|--------------------------------------|----------------------|----------|----------|---------------|----------------------------|---|
| | List | | | | | | |
| Application | Required List | Configure | | X | Add Packages | | List of applications that the user cannot uninstall. |
| Container Password Restriction | Min Mutation on Change | 0- | | X | | | Minimum number of characters that must be changed when container password is changed. |
| Container Password Restriction | Minimum Length | 0- | | X | 6 | KNOX-29-014900 | Minimum container password length. |
| Container Password Restriction | Max Time to Lock | 0- | | X | 15 | KNOX-29-015100 | Minutes of inactivity after which container will lock. |
| Container Password Restriction | Maximum Failed Attempts | 0- | | X | 10 | KNOX-29-015200 | Unsuccessful login attempts before container admin lock. |
| Container Restriction | Web Proxy | Configure | X | | Add Web Proxy | KNOX-29-013500 | IP address and port of the DoD proxy. |
| Container Restriction | Password complexity | Alphanumeric Complex | | X | Alphanumeric | | |
| Container Restriction | Allow camera | Enable / Disable | | X | | | Camera use inside container. |
| Container Restriction | Allow account addition | Enable / Disable | | X | | | Email accounts inside container. |
| Container Restriction | Allow share via list | Enable / Disable | | X | | | Share via list option inside container applications. |
| Container Restriction | Allow contact info outside container | Enable / Disable | | X | Enable | | Sharing of container contacts to outside contacts. |

UNCLASSIFIED

Samsung Android (with Knox 1.x) Configuration Table, V2R1
17 April 2014

DISA Field Security Operations
Developed by Samsung and DISA for the DoD

| Policy Group | Policy Rule | Options | Required | Optional | Settings | Related Requirement Number | Comments |
|-----------------------|---------------------------------------|------------------|----------|----------|----------|----------------------------|--|
| Container Restriction | Allow cookies | Enable / Disable | | X | | | Container native browser application only. |
| Container Restriction | Enable auto-fill | Enable / Disable | | X | | | Container native browser application only. |
| Container Restriction | Enable JavaScript | Enable / Disable | | X | | | Container native browser application only. |
| Container Restriction | Enable popups | Enable / Disable | | X | | | Container native browser application only. |
| Container Restriction | Enable CAC authentication for email | Enable / Disable | | X | Enable | | For native email client inside container. |
| Container Restriction | Enable CAC authentication for browser | Enable / Disable | | X | Enable | | Container native browser application only. |

APPENDIX C. APPLE IOS 6 VPN CONSIDERATIONS

VPN considerations are taken from Apple iOS 6 STIG Overview developed by DISA (2013, p. 13).

UNCLASSIFIED

Apple iOS 6 STIG Overview, V1R2
9 May 2013

DISA Field Security Operations
Developed by DISA for the DoD

2.7 VPN Considerations

Current DoD mobile device implementations use mobile device management products that transfer data between the mobile device and the DoD network via a secure connection between the management agent on the mobile device and the management server located on the DoD network. This type of connection usually requires a vendor-managed mobile device traffic router so only outward bound (from the server) connections are used to set up the connection between the mobile device and server (a DoD security requirement). (See Figure 2-1 for an example of this type of mobile device management implementation.) These types of connections have additional limitations, including difficulty in setting up secure connections to back-office servers and lack of CAC proxy support by the management server (required so the device user can CAC authenticate to the DoD network or to a back-office server).

The DoD is currently exploring session-based mobile VPNs as an alternate method for setting up secure connections between mobile devices and DoD networks. There are both advantages and disadvantages for mobile VPNs.

Advantages

- Supports routing all mobile device Internet traffic through the DoD Internet gateway.
- Supports easy access to DoD network servers.
- Supports easy user authentication to the network.

Disadvantages

- Currently available mobile VPN products do not support both FIPS-validated encryption and CAC authentication.
- Limited choices available today for session-based VPNs. (IPSec VPNs have significant performance issues in a handheld mobile device environment.)
- The Wireless STIG requires mobile VPN clients to drop connections to DoD networks after a period of user inactivity. This requirement could cause performance issues in an environment with push email service and CAC authentication. Testing is required to determine the extent of these issues.
- Currently available mobile VPN products do not support saving downloaded data to the security container.

2.8 Public Key Infrastructure (PKI) Support

DoD PKI-issued digital certificates are used to digitally sign and encrypt emails. The use of software certificates on DoD smartphones is not currently authorized by DoD policy and is not supported by the DoD PKI Office.

2.9 Disposal of iOS-Based Devices

Appendix B provides required sanitization procedures to follow prior to disposing of iOS devices.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- Barker, E. (2014, February 13). Navy e-Learning now offers direct access Navy education and Training Command Public Affairs. NNS140213-19. Retrieved from http://www.navy.mil/submit/display.asp?story_id=79125
- Biometers Associates, LP. (n.d.). BaiMobile 301MP, 301MP-LT, & 3000MP Bluetooth Smart Card Reader specifications. Retrieved September 15, 2014 from <http://www.baimobile.com>
- Defense Information Systems Agency. (n.d.-a). Department of Defense Mobility Program. Retrieved September 22, 2014, from <http://www.disa.mil/Services/Enterprise-Services/Mobility>
- Defense Information Systems Agency. (n.d.-b). Secure unclassified mobile devices and wireless services. Retrieved from <http://www.disa.mil/Services/Enterprise-Services/Mobility/Devices-and-Wireless-Services>
- Defense Information Systems Agency. (2010, October 29). *Access control in support of information systems*. STIG V2R3. Fort Meade, MA: Author.
- Defense Information Systems Agency. (2013, May 9). *Apple iOS 6 security technical implementation guide (STIG) overview V1R2*. Washington, DC: Author.
- Defense Information Systems Agency. (2014a, May 14). Announces DoD mobility capability, 2.0 for Android/Samsung KNOX. Press release. Retrieved from <http://www.disa.mil/News/PressResources/2014/Mobility-Android-Samsung>
- Defense Information Systems Agency. (2014b). *Joint information environment DISA strategic plan 2014–2019*. Retrieved August 13, 2014 from <http://www.disa.mil/~media/Files/DISA/About/Strategic-Plan.pdf>
- Department of Defense. (2007). *Information assurance*. DODI 8500.01E <http://dodcio.defense.gov/Portals/Documents/DIEA/850001p.pdf>
- Department of Defense. (2008). *Clearance of DOD information for public release*. DODD 5230.09. <http://www.dtic.mil/whs/directives/corres/pdf/523009p.pdf>
- Department of Defense. (2011). *Public key infrastructure (PKI) and public key (PK) enabling*. Instruction 8520.2. Washington, DC: Author. <http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf>
- Department of Defense. (2012a). *Department of Defense mobile strategy* [memorandum]. Washington, DC: Author

Department of Defense. (2012b). *DoD Information Security Program: Controlled unclassified information (CUI)*. DOD Instruction 5200.01, Vol. 4. Washington, DC: Author.

Department of Defense. (2012c). *DoD Information Security Program: Overview, classification, and declassification*. DODI 5200.01, Vol. 1. Washington, DC: Author.

Department of Defense. (2013, February 15). *Department of Defense commercial mobile device implementation plan* [memorandum]. Washington, DC: Author.

Federal Information Security Management Act, Pub. L. No. 107-347, 44 U.S.C., §. 3542 (2002).

National Institute of Standards and Technology. (2004, February). *Standards for security categorization of federal information and information systems*. FIPS 199. Washington, DC: Author. Retrieved from <http://www.csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>

Samsung & Defense Information Systems Agency. (2014a, April 17). *Samsung Android (with Knox 1.x) security technical implementation guide (STIG) overview*. V2R1. Washington, DC: Defense Information Systems Agency.

Samsung & Defense Information Systems Agency. (2014b, April 17). *Samsung Android (with Knox 1.x) STIG configuration table*. V2R1. Washington, DC: Defense Information Systems Agency.

Samsung. (n.d.). Samsung KNOX 2.0: The evolution of enterprise mobility. Retrieved August 11, 2014, from <http://www.samsung.com/global/business/mobile/platform/mobile-platform/knox/>

Secure unclassified mobile devices and wireless services. (n.d.). Retrieved July 9, 2014, from <http://www.disa.mil/Services/Enterprise-Services/Mobility/Devices-and-Wireless-Services>

Thursby Software Systems, Inc. (2014, October 16). PKard Reader bundled reader, software & support for iPad, iPhone, & iPod specifications. Retrieved September 12, 2014 from <http://www.thursby.com/products/pkard-reader>

VMware Horizon. (2014, September) Using VMware Horizon Client for iOS EN-001481-01. Retrieved October 15, 2014 from <http://www.vmware.com/support/pubs>

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California